1/2015

Datenschutz Nachrichten

38. Jahrgang
ISSN 0137-7767
12,00 Euro



Mobilität, Telematik und Datenschutz

■ Mein Auto ist ein mieser Verräter!? ■ PKW-Maut-Systeme in Europa ■ Das Kfz, die Telematik und der Datenschutz ■ Roboter auf Rädern ■ eCall-Systeme ■ Belohnung für vorbildliche Autofahrer ■ Die Smartifizierung der beruflichen Mobilität ■ Die CDU/CSU und der Datenschutz ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Dr. Stefan Brink
Mein Auto ist ein mieser Verräter!? 4

Frank Spaeing
PKW-Maut-Systeme in Europa 8

Thilo Weichert
Das Kfz, die Telematik und der Datenschutz 10

Snoopy
Roboter auf Rädern – eine leise Polemik wider den Markt 16

Franziska Facius
Die Verordnung der Regeln über die Einführung von bordeigenen eCall-Systemen in Fahrzeugen – ein Datenschutz-Papiertiger? 20

Christian Siedenbiedel
Belohnung für vorbildliche Autofahrer 24

Maria Koch – Lea Rothmann
Privatheit verhandeln
Die Smartifizierung der beruflichen Mobilität 26

BfDI Pressemitteilung
Andrea Voßhoff stellt Datenschutzinformationen in neuem Format vor. Thema der ersten Ausgabe: Datenschutz im Auto 28

Klaus-Jürgen Roth
Die CDU/CSU und der Datenschutz 29

Datenschutznachrichten

Datenschutznachrichten aus Deutschland 32

Datenschutznachrichten aus dem Ausland 39

Technik-Nachrichten 44

Soziale Medien 46

Rechtsprechung 47

Normentwurf „Leitlinie Löschkonzept“ 52

Buchbesprechungen 52

Termine

Freitag, 17. April 2014, 18:00 Uhr
BigBrotherAwards
Verleihung der Negativ-Preise für Datenkraken
Bielefeld, Hechelei
http://www.bigbrotherawards.de

Samstag, 18. April 2015, 13:30 – 18:30 Uhr
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle.
dvd@datenschutzverein.de

Freitag, 01. Mai 2015
Redaktionsschluss DANA 2/2015
Thema: Flüchtlinge und Datenschutz

Samstag, 04. Juli 2015, 11:00 – 15:00 Uhr
DVD-Vorstandssitzung
Berlin. Anmeldung in der Geschäftsstelle.
dvd@datenschutzverein.de

Freitag, 09. Oktober 2015
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle.
dvd@datenschutzverein.de

Freitag, 09. Oktober 2015 – Samstag, 10. Oktober 2015
DVD-Jahrestagung in Bonn
Thema: Mobilität und Telematik (Arbeitstitel)

Sonntag, 11. Oktober 2015
DVD-Mitgliederversammlung in Bonn



Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
38. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Karin Schuler, Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

Editorial

Liebe Leserinnen und Leser,

Als wir 2014 den Schwerpunkt „Mobilität, Telematik und Datenschutz" für die DANA 1/2015 festlegten, war die heutige Popularität des Themas nicht absehbar. Es scheint geradezu, als wären Automobilhersteller, Datenschutzbeauftragte, Automobilclubs, Konferenzveranstalter, Forschungsgruppen und die EU innerhalb des letzten Jahres plötzlich alle auf einen ständig mehr Fahrt aufnehmenden Zug aufgesprungen, der uns Anfang letzten Jahres noch wie eine Bimmelbahn erschien. Dass man heute schon fast von einem Hype sprechen kann, liegt vermutlich an vielen Faktoren. Auch wenn nicht alle nur mit Datenschutz zu tun haben, werden Mobilität und Datenschutz aus sehr unterschiedlichen Blickwinkeln und vielen gesellschaftlichen Gruppierungen beleuchtet.

Zu unserer Freude hatten wir daher keine Probleme, für diese Ausgabe eine ganze Reihe kompetenter Autorinnen und Autoren zu gewinnen. Thilo Weichert, Stefan Brink und Frank Spaeing verschaffen zunächst den notwendigen Überblick über Datenverarbeitung im Auto und beim Autofahren. Es folgen Artikel zum Status des EU-Vorhabens eCall (Francisca Facius), eine Beschreibung der auf Black Boxes beruhenden Versicherungstarife (Christian Siedenbiedel) und ein Bericht zum Projekt eFahrung (Koch/Rothmann). Snoopy steuert die spöttisch-verzweifelte Sicht des Technikers bei und außerhalb des Schwerpunktthemas befasst sich Klaus-Jürgen Roth mit parteipolitischen Haltungen zum Datenschutz. Deutsche und internationale Datenschutznachrichten finden Sie, wie gewohnt, in der entsprechenden Rubrik.

Dieses Schwerpunktheft soll auch eine Einstimmung für die im Oktober geplante Jahrestagung der DVD zum gleichen Thema sein. Wir wünschen Ihnen viel Vergnügen und Erkenntnis bei der Lektüre und würden uns freuen, Sie im Oktober in Bonn begrüßen zu können.

Karin Schuler und Frank Spaeing

Autorinnen und Autoren dieser Ausgabe:

Dr. Stefan Brink
Leiter Datenschutz in der Privatwirtschaft beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz. s.brink@datenschutz.rlp.de

Franziska Facius
arbeitet als Rechtsanwältin. Bloggt über Recht und Unrecht im Netz. facius@netzrecht-blog.de

Maria Koch
(Mag. phil.) ist studentische Mitarbeiterin am Institut für Soziologie, Fachgebiet Planungs- und Architektursoziologie. Sie beschäftigt sich vor allem mit Stadtforschung und Frauen- und Geschlechterstudien sowie Partizipations- und Beteiligungsformen in der Stadtentwicklung.
Sie ist unter der E-Mail m.koch@campus.tu-berlin.de zu erreichen.

Klaus-Jürgen Roth
roth@datenschutzverein.de

Lea Rothmann
(Dipl.-Soz.) ist wissenschaftliche Mitarbeiterin im Forschungsprojekt „eFahrung. Unternehmensübergreifende Nutzung von E-Fahrzeugen in Unternehmensflotten" und Doktorandin am Institut für Soziologie, Fachgebiet Planungs- und Architektursoziologie. Sie beschäftigt sich mit der Eigenlogik von Städten und Raumwahrnehmung. Sie ist unter der E-Mail lea.rothmann@tu-berlin.de zu erreichen.

Christian Siedenbiedel
Jahrgang 1969, ist Wirtschaftsredakteur der Frankfurter Allgemeinen Zeitung. Er schreibt über Finanzthemen, die Bahn und Geldpolitik.

Snoopy
selbständiger IT-Berater mit Schwerpunkt IT-Security, hält div. Vorträge und schreibt Glossen und Fachartikel. snoopy@snoopix.de

Frank Spaeing
Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz e.V.. spaeing@datenschutzverein.de

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel.
weichert@datenschutzzentrum.de

Dr. Stefan Brink

Mein Auto ist ein mieser Verräter!?

Das vernetzte Auto als Herausforderung für den Datenschutz


Bild: ClipDealer.de

Das Thema Car-2-Car-Kommunication und Datenschutz entwickelt sich immer mehr zu einer der zentralen Fragestellungen im Bereich der informationellen Selbstbestimmung. Das hängt zum einen damit zusammen, dass – zumal in Deutschland – das Auto als „letzte Insel der Privatheit“[1] angesehen wird. Das Automobil bildet eine auch emotional aufgeladene Synthese aus Eigentum und Freiheit (Roßnagel) und stellt andererseits einen der wenigen verbliebenen Ruhe- und Rückzugsräume dar. Gleichzeitig wird das vernetzte Kfz aber in seiner immer tiefer gehenden Vernetzung zum Standardmodell für das „Internet der Dinge“: Nicht der Kühlschrank, auch nicht unbedingt das Smartphone, sondern das vernetzte Automobil fokussiert damit alle Hoffnungen und Ängste, die mit dem Internet der Dinge verbunden werden. Im Jahr 2016 sollen 80% der weltweit verkauften Neufahrzeuge bereits vernetzt sein.[2] Das Überwachungs- und Ausforschungspotenzial von Fahrzeugdaten ist dabei unbestritten. Jim Farley, Marketingchef von Ford, brachte es auf der Consumer Electronics Show CES 2014 in Bezug auf den sensiblen Informationsgehalt von Fahrzeugdaten auf den Punkt: „Wir kennen jeden Autofahrer, der die Verkehrsregeln bricht. Und wir wissen, wo und wie jemand das tut.“[3] Daher ist es kein Wunder, dass der Big Brother Award 2014 in der Kategorie Technik an „die Spione im Auto“ ging. Dieser „Oskar für Datenkraken“ ließ sich in diesem Fall jedoch nicht an einen konkreten „Schuldigen“ für die Verletzung der Privatsphäre verleihen, sondern ging an die „unbekannte Vielzahl“ von Herstellern von Kraftfahrzeugen, Zulieferern, Werkstätten – und nicht zuletzt an den Gesetzgeber.

1. Wer bringt das Auto zum Reden?

a) Es ist der massiven Fortentwicklung der Fahrzeugsensorik zu verdanken, dass wir es mittlerweile mit einer Vielzahl von Fahrzeugdaten zu tun haben, die uns nicht nur Auskunft geben über den Standort des Fahrzeugs, seine Geschwindigkeit und Fahrtrichtung. Zu den Datensammlern zählt etwa auch die Videoüberwachung an Front oder Heck des modernen Fahrzeugs, auch die Audioüberwachung des Innenraums, und natürlich die gesamte Kfz-Sensorik einschließlich der Motorelektronik misst fleißig und unaufhörlich.

Neben diesen Betriebsdaten machen sogenannte „Komfortdaten“ aus dem Bereich der Fahrzeugconvenience mittlerweile die große Masse der anfallenden Daten aus. Hierzu zählen die Fahrzeugkommunikation mittels Kfz-eigener SIM-Card, aber auch das Cockpit Entertainment, die auf den jeweiligen Fahrer abgestimmte Standardeinstellung von Sitz, Lenkradhöhe, der bevorzugte Fahrstil und natürlich der Musikgeschmack samt einschlägigen Internet-Links.

b) Für Datenschützer stehen natürlich die personenbezogenen Informationen im Vordergrund: Moderne Fahrzeuge überwachen heute nicht nur den Betriebszustand des Kfz, sondern auch den „Systemzustand“ des Fahrers. Bei Daimlers „Attention Assist“ etwa wertet ein Algorithmus das Lenkverhalten des Fahrzeugführers aus. Kommt er zum Schluss, dass die Konzentration des Fahrers nachlässt, wird dieser aufgefordert, eine Kaffeepause einzulegen.[4] Aber auch „technische Betriebsdaten“ sind in aller Regel zumindest personenbeziehbar, etwa wenn sie mit einer Fahrzeugidentitätsnummer und somit zugleich dem Fahrzeughalter verknüpfbar sind.

c) Vieles dieser Fahrzeugsensorik richtet sich nach den Ausstattungswünschen des Kfz-Halters, ist also so gesehen „freiwillig“ installiert; manches aber – wie etwa die auf europäischer Ebene eingeführte Rettungskommunikation eCall – wird bis ins Jahr 2018 verpflichtend implementiert werden; andere Datensensoren, wie etwa im Bereich der Abgasmessung, sind dies bereits.

eCall verdient dabei besondere Aufmerksamkeit: Das automatische Notrufsystem setzt bei Unfällen selbstständig einen Notruf ab und übermittelt die hierfür erforderlichen Unfalldaten (insbesondere die Koordinaten des Unfallorts, den Unfallzeitpunkt und Daten zu den gemessenen Aufprallkräften) über eine eigene SIM-Card via Mobilfunknetz direkt an eine Notrufzentrale. Die Bedeutung von eCall erschöpft sich dabei keineswegs in seiner Funktion als Rettungsassistenzsystem; offenkundig verfolgt die EU-Kommission damit auch die industriepolitische Zielsetzung,

hierüber einen technischen Einstieg für die Vernetzung von Autos insgesamt zu schaffen. Auf dieser Plattform werden nämlich zukünftig „innovative Mehrwertdienste“ andocken. eCall wird damit zugleich zum Türöffner für Big Data im Fahrzeugbereich.

d) Die Zahl der Assistenzsysteme, die für den Fahrzeugführer und die Insassen die Benutzung des Kfz sicherer und angenehmer machen sollen, nimmt dabei stetig zu: Gestern waren es Tempomat und ESP, heute sind dies Müdigkeitswarner und Spurassistent und übermorgen bereits das selbstfahrende „autonome“ Automobil. Bei genauerer Betrachtung verliert der Fahrer schon heute die Kontrolle über sein Fahrzeug, wenn ESP und ABS zum Einsatz kommen. Diese Programme kann der Fahrer nicht mehr übersteuern – das autonome Fahren ist also keine reine Zukunftsmusik mehr.

Mehr als 80 Steuergeräte finden wir heute in modernen Bordnetzen. Bereits jetzt ist absehbar, dass sich die mengenmäßige Zunahme im Bereich der Kfz-Sensorik ungebremst fortsetzen wird. Seit September 2014 müssen etwa Neufahrzeuge in den USA einen Event Data Recorder mit sich führen, der nach dem Vorbild von Flugdatenschreibern unfallrelevante Parameter aufzeichnet und für die Unfallrekonstruktion vorhält. Zusatzangebote wie eigene „Vehicle homepages“, die insbesondere im Bereich elektrisch betriebener Fahrzeuge zum Angebotsumfang der Hersteller zählen, gesellen sich hinzu und runden das „Kfz-Daten-Paket“ ab.

e) Die Kommunikationswege des vernetzten Automobils sind denkbar vielfältig. Bei Car-2-Car-Kommunikation findet der Informationsaustausch zwischen Automobilen statt, etwa über die Geschwindigkeit, die Richtung oder den Einsatz des ABS-Systems des Fahrzeugs. Dies hilft dabei, Unfälle zu verhindern, über Notbremsungen vorausfahrender Fahrzeuge zu informieren oder Hinweise auf Glatteis- oder Aquaplaning-Gefahren an nachfolgende Verkehrsteilnehmer weiterzuleiten. Die Car-2-X-Kommunikation bezieht darüber hinaus die gesamte Verkehrsinfrastruktur in die Datenströme mit ein. Hier werden Informationen ausgetauscht über Verkehrsflüsse, Ampelschaltungen, aber auch aggregierte Angaben über die Positionen weiterer Verkehrsteilnehmer.[5] Jedes Fahrzeug ist dabei Sender und Empfänger zugleich, viele Verkehrssysteme werden für ihre volle Funktionstüchtigkeit nicht auf die freiwillige Einwilligung, sondern auf eine verpflichtende Teilnahme setzen. Die Sicherheit und Leichtigkeit des Straßenverkehrs werden die schlagenden Argumente dafür sein, die Gesamtheit der Kfz-Nutzer in eine Daten-Lieferpflicht einzubeziehen.

2. Mein Auto – meine Daten?

a) Das Interesse an diesen Fahrzeugdaten ist ungebremst, die Schar der Interessenten kaum überschaubar: Da ist natürlich zunächst einmal der Fahrzeugführer, aber auch ein hiervon möglicherweise zu unterscheidender Fahrzeughalter und -eigentümer. Da ist der Fahrzeughersteller, der Fahrzeugdaten im Rahmen seiner Garantieverpflichtung oder für mögliche Produkthaftungsfälle begehrt. Da sind Wartungsdienstleister, die – ggf. unabhängig vom Fahrzeughersteller – Daten über die Fahrzeugnutzung sinnvoll verwerten können. Daneben sind auch Unfall-, Wert- und Verkehrssachverständige an der Nutzung der Fahrzeugdaten interessiert, teilweise sogar darauf angewiesen. Auch weitere Dritte, seien es andere Verkehrsteilnehmer oder Gewerbetreibende aus der Versicherungs- oder Marketingbranche, wünschen Zugang zu den Fahrzeugdaten. Mit besonderem Nachdruck greifen Sicherheitsbehörden wie die Polizei, Zivil- und Strafgerichte, aber auch Sicherheitsdienstleister wie der TÜV oder Infrastrukturbehörden zum Zwecke der Mautberechnung oder der Verkehrslenkung nach diesen Fahrzeugdaten.

b) Die Frage „Wem gehören die Fahrzeugdaten?“ stellte der 52. Deutsche Verkehrsgerichtstag im Januar 2014 in Goslar. Er plädierte dafür, das informationelle Selbstbestimmungsrecht durch Transparenz und Wahlfreiheit der betroffenen Fahrzeughalter und Fahrer zu sichern. Die in diesem Zusammenhang immer wieder aufgeworfene Frage nach den Eigentumsverhältnissen an den Fahrzeugdaten ist allerdings aus Perspektive der Datenschützer weniger relevant als man meinen könnte. Natürlich kann man die zivilrechtliche Fragestellung, ob dem Hersteller Einzelangaben aus dem Bereich der Motorsteuerung rechtlich „zustehen“ – auch etwa unter dem Gesichtspunkt des Urheberrechts oder zum Schutz von einschlägigen Geschäfts- und Betriebsgeheimnissen – erörtern und klären. Für Datenschützer ist jedoch nicht die Frage nach den Eigentumsverhältnissen, sondern die Frage nach der Personenbeziehbarkeit der Fahrzeugdaten der entscheidende Aspekt.

Auch wenn bestimmte Fahrzeugdaten im Privateigentum des Kfz-Eigentümers, des Herstellers oder eines Versicherungsunternehmens, das eigene Datensensorik im Fahrzeug installiert hat, stehen sollte, der Datenschützer fragt unabhängig von diesen möglichen Rechtsverhältnissen nach der Befugnis einer verantwortlichen Stelle zum Erheben, Speichern, Übermitteln oder Nutzen dieser Fahrzeugdaten (vgl. § 3 BDSG). Der Nachdruck, mit dem mittlerweile die Debatte um „data ownership“ und die informationellen Eigentumsverhältnisse in Bezug auf die Fahrzeugdaten geführt wird, lässt allerdings den Eindruck entstehen, dass es hier weniger um die Suche nach rechtswissenschaftlicher Erkenntnis, als um den Versuch geht, den Datenschutz durch eine vermeintlich relevante Debatte um das „Dateneigentum“ an die Seite zu drängen. Die Reaktion des Datenschutzes sollte hier eindeutig sein: Eigentumsverhältnisse sind nicht relevant für die Frage, ob Daten personenbezogen und damit schutzwürdig sind. Wer den Datenschutz unter Eigentumsvorbehalt stellt, legt die Axt an die verfassungsrechtlich garantierte informationelle Selbstbestimmung.

3. Zum Personenbezug von Fahrzeugdaten

Zutreffend konstatiert die Fraktion Bündnis 90/Die Grünen im Bundestag in ihrer kleinen Anfrage an die Bundesregierung[6] zum Datenschutz im Auto: „Die vollständige Erfassung der Mobilität von Personen liefert zugleich Teilbilder der Persönlichkeit, zentraler persönlicher Präferenzen und Interessen, welche die Verbraucherinnen und

Verbraucher womöglich lieber für sich behalten wollen.“ Demgegenüber wird von Herstellerseite immer wieder betont, dass es im Bereich der Fahrzeugsensorik um „rein technische Datenverarbeitung“ ginge, die überhaupt keinen Personenbezug aufweise und daher datenschutzrechtlich irrelevant sei.

Dies ist regelmäßig nicht der Fall: Wer sich die bei Betrieb und Nutzung von Kraftfahrzeugen anfallenden Datenpakete im Einzelnen anschaut, wird feststellen, dass regelmäßig die Fahrzeugidentitätsnummer (FzID) mit den Sensorikdaten verknüpft ist und sich diese Daten aufgrund weiterer Verknüpfungsmöglichkeiten zwar nicht für jedermann, aber doch für manche verantwortliche Stelle mit der Person des Halters, ggf. auch mit der des Fahrers, verbinden lassen. Mehr setzt § 3 Abs. 1 BDSG für personenbezogene Daten aber auch nicht voraus, insbesondere kommt es weder auf eine besondere „Persönlichkeitsrelevanz“ der Daten noch auf deren wirtschaftliche Verwertbarkeit an. Jedenfalls dann, wenn diese Sensorikdaten gesammelt und aggregiert verarbeitet werden, gewinnen sie eine inhaltliche Aussagekraft, die sie zu Einzelangaben über persönliche bzw. sachliche Verhältnisse einer bestimmten oder zumindest bestimmbaren Person und damit regelmäßig zu personenbezogenen Daten im Sinne von § 3 Abs. 1 BDSG machen. Selbst bei wechselnden Fahrzeugführern werden diese Daten immer einen Bezug zum Fahrzeughalter aufweisen. Auch weitere Fahrzeuginsassen oder Straßenpassanten, die optisch und akustisch von der Fahrzeugsensorik erfasst werden und mit Lokalisationsdaten oder „Komfortdaten“ wie Fahrstil oder Musikgeschmack in Verbindung gebracht werden, sind „Betroffene“ im Sinne der Legaldefinition des § 3 Abs. 1 BDSG.

4. Überlegungen zum Datenschutz

a) In mehreren Studien im Rahmen des Forschungsprojekts „Fueling the connected car“ des Lehrstuhls für Innovation, Strategie und Organisation der RWTH Aachen wurde deutlich, dass Privatsphärebedenken im Kontext des vernetzten Fahrzeugs sehr präsent sind: 49% der befragten Autofahrer gaben an, dass sie die eigene Privatsphäre bei einer Nutzung ihrer Fahrdaten grundsätzlich bedroht sehen.[7] Die Position der deutschen Bundesregierung zum Einsatz moderner Datenverarbeitungssysteme in Kraftfahrzeugen ist demgegenüber denkbar neutral: „Der entsprechende Nutzen ist im Einzelfall mit etwaigen datenschutzrechtlichen Risiken abzuwägen. Datenschutzrechtliche Vorgaben sind zu beachten.“[8] Ratlos ist die Bundesregierung auch bei der Anwendung des datenschutzrechtlichen Instrumentariums auf moderne Fahrzeugtechnik: „Wer verantwortliche Stelle und Betroffener ist, ist in jedem konkreten Einzelfall zu ermitteln und lässt sich nicht pauschal beantworten. In mehrpolaren Verhältnissen – etwa einem Kfz-Hersteller, einem Halter, einem Fahrer, einer Werkstatt, einem Verkehrsdienst-Anbieter etc. – ist die Zuordnung häufig äußerst schwierig.“[9]

b) Die Fülle der neu aufgetretenen Datenschutzfragen ist tatsächlich nahezu unüberschaubar: Eine Einwilligungserklärung, die der Fahrzeughalter beim Fahrzeugkauf ausdrücklich – oder noch problematischer: per AGB – abgibt, gilt sicherlich datenschutzrechtlich nicht für den jeweiligen Fahrzeugnutzer. Wie aber könnte dieser dem Halter und dem Hersteller seine Zustimmung zu Datenverwendungen erklären? Ist bei Mietfahrzeugen als zwingende technisch-organisatorische Maßnahme im Sinne von § 9 BDSG eine Löschvorrichtung für Adressangaben in Navigationsgeräten, gewählte Telefonnummern, Spracheingaben in Freisprecheinrichtungen oder Nutzungsdaten zum Kfz-Infotainment-System vorzusehen? Noch grundsätzlicher: Ist das BDSG anwendbar, wenn ein Kraftfahrzeug mitsamt seinen Datenspeichern zwischen zwei Privatleuten veräußert wird? Oder gilt da die den Anwendungsbereich des BDSG restringierende Vorschrift des § 1 Abs. 2 Nr. 3, wonach das BDSG für persönliche oder familiäre Tätigkeiten nicht gilt?

Ebenfalls neuartig sind diese Problemstellungen: Das vernetzte Fahrzeug ist zwar eine rollende Datenbank, viele Fahrzeugdaten sind jedoch auch für die verantwortliche Stelle (also etwa für den Fahrzeughersteller) nicht unmittelbar verfügbar. Zahlreiche Fahrzeugspeicher sind nur vor Ort, also etwa im Rahmen eines Werkstattbesuchs, auslesbar und bis dahin auch nicht für die verantwortliche Stelle erheb- und nutzbar. Umgekehrt hat der Fahrzeugführer zwar die tatsächliche Herrschaft über die Datenspeicher des von ihm geführten Fahrzeugs, kann diese jedoch aus technischen Gründen weder auslesen noch nutzen. Die hierfür notwendigen Gerätschaften werden dem Fahrzeugführer in aller Regel auch nicht zur eigenen Verwendung zur Verfügung gestellt. Kenntnis von gespeicherten Daten bekommt er daher immer nur durch die verantwortliche Stelle selbst oder durch Dritte (etwa Vertragswerkstätten), die aber zugleich eigene Interessen an den Fahrzeugdaten haben und damit nicht gerade ideale Mittler sind. Die Fahrzeughersteller werden gut daran tun, die derzeit bestehende Informationsasymmetrie zu Lasten der Fahrer und Halter durch selbstgesetzte faire Regeln aufzuheben.

c) Gerade der Umfang der eingesetzten Fahrzeugsensorik und die Fülle an Daten, die bei jeder Nutzung des Fahrzeuges anfallen, lassen schon heute die Anlage sogenannter „Fahrerprofile“ als möglich und durchaus erwartbar erscheinen. Hiermit verbindet sich aus Datenschutzsicht unmittelbar das Gebot der Sensibilität im Umgang mit solchen Fahrzeugdaten. Erscheint angesichts solcher Big Data-Anwendungsfälle das traditionelle datenschutzrechtliche Gebot der Datensparsamkeit (§ 3a BDSG) auch als reichlich antiquiert, um gültiges Recht handelt es sich nach wie vor.

d) Vollständig aktuell sind demgegenüber die Folgerungen, die sich aus dem informationellen Selbstbestimmungsrecht des Fahrzeugführers und -halters ergeben. Hierzu zählt etwa die gebotene Aufklärung über automatisierte Datenerhebungen und Datenverarbeitungen des Kfz, die bereits beim Fahrzeugkauf stattfinden muss. Die Erfahrung zeigt allerdings, dass solche Aufklärungspflichten gerne hintangestellt und im Rahmen des „lästigen Papierkrams“ über AGBs abgewickelt werden. Dies wird der Bedeutung, welche die Fahrzeugdaten für den Betroffenen zukünftig aber auch für die Fahrzeughersteller haben, in keiner Weise gerecht.

An dieser Stelle sind übrigens auch Private angesprochen, die ihr sensorisch aufgerüstetes Fahrzeug anderen zur Nutzung überlassen. Aus dem Grund-

recht auf informationeller Selbstbestimmung ergibt sich auch das (jedenfalls an den Gesetzgeber gerichtete) Gebot, die Datensouveränität des betroffenen Fahrers bzw. Halters zu achten. Im Rahmen des technisch Machbaren müssen die Betroffenen daher in die Lage versetzt werden, unerwünschte Datenerhebungen zu verhindern und erhobene Daten aufgrund eigener Entscheidung zu löschen. Dies setzt insbesondere voraus, dass die Hersteller Datenverarbeitungsalternativen bei der Fahrzeugsensorik vorsehen und – so die Forderungen des Privacy by Design – differenzierte Verarbeitungsmodalitäten insbesondere für besonders sensible Daten vorsehen, Verschlüsselungsmöglichkeiten nutzen und durch intelligente (datenschutzfreundliche) Standardeinstellungen (Privacy by Default) favorisieren. Darüber hinaus müssen sämtliche verantwortliche Stellen, die personenbezogene Fahrzeugdaten erheben oder darauf zugreifen müssen, ihrerseits dafür Rechnung tragen, dass die gesetzlichen Auskunftsrechte (§ 34 BDSG) und die Löschansprüche (§ 35 BDSG) ausgeübt und durchgesetzt werden können.

e) Dies gilt keineswegs nur für das nicht-öffentliche Datenschutzrecht unter Privaten, sondern auch für die gesetzlichen Datenschutzpflichten öffentlicher Stellen. Kann die Polizei bei der Aufklärung eines Unfalls auf die Daten des ABS-Steuergeräts, den Speicher des Navigationssystems oder auf Daten der Motorsteuerung zugreifen, so ist die Rekonstruktion von Fahrzeugposition, Fahrzeuggeschwindigkeit und Bremsmanövern ein wichtiger Beitrag zur Aufklärung des Unfallgeschehens. Da aber kein Fahrzeugführer an der Aufklärung seines Fehlverhaltens mitwirken muss (hier gilt der verfassungsrechtliche Grundsatz der Selbstbelastungsfreiheit „nemo tenetur"), wäre die Löschung dieser Fahrzeugdaten vor dem Polizeizugriff rechtlich durchaus zulässig. Ein „Panik-Knopf", mit dem der Fahrzeugführer sämtliche Datenspeicher seines Kfz löscht, wenn er eine Kontrollsituation auf sich zukommen sieht, steht dem Verfassungsrecht jedenfalls näher als die Auffassung, der potenzielle Rechtsverletzer dürfe die staatlichen Ermittlungsbehörden und Gerichte nicht an ihrer Arbeit hindern oder diese durch Datenlöschungen erschweren. Bei den Datenschutzaufsichtsbehörden mehren sich jedenfalls die Nachfragen besorgter Werkstätten, ob sie ohne Verletzung der Rechte des Fahrzeughalters von der Staatsanwaltschaft beschlagnahmte Fahrzeuge „auslesen" dürfen. Zumindest die Sensibilität der Kfz-Werkstätten ist aus Sicht der Aufsichtsbehörden uneingeschränkt zu begrüßen.

Dennoch: Die auch in Europa angedachten Unfalldatenspeicher werden durch eine nachvollziehbare Regelung des Zugriffsregimes „abgefedert" werden müssen, um vom Fahrer nicht als vorweggenommene Selbstbelastung empfunden zu werden. Der Traum von Freiheit, den Mobilität nach wie vor in sich birgt, ist ausgeträumt, wenn das eigene Fahrzeug als „Verräter" verstanden wird.

5. Erstes Resümee

Die Vor- und Nachteile von Big Data im Automobil liegen auf der Hand: Den klaren Fortschritten bei der Verkehrssicherheit lässt sich wenig entgegensetzen – wieder mal sehen sich Datenschützer der Eingängigkeit von Sicherheitsargumentationen gegenüber. Zur Erhöhung von Verkehrssicherheit gesellt sich die Steigerung der Verkehrseffizienz, auch dies ein gewichtiges Argument für das vernetzte Auto. Weitere Vorteile des *connected car* sind ebenfalls unbestreitbar: Eine Auswertung der jetzt zur Verfügung stehenden Datenmengen ermöglicht etwa die individuelle Berechnung von Serviceintervallen, welche Parameter wie Nutzungshäufigkeit oder den persönlichen Fahrstil für eine optimale Taktung des Fahrzeugservices nutzt. Umgekehrt können Fahrzeughersteller auch bei der Entscheidung über Gewährleistungsansprüche oder die Zubilligung von Kulanzleistungen auf die Fahrzeugdaten zurückgreifen und „Informationsvorsprünge" des Fahrzeughalters abbauen. So wird vom Fall eines Münchener Cabrio-Besitzers berichtet, der sich wegen eines Fehlers beim Schließmechanismus des Cabrios auf einen Garantiefall berief, von seinem eigenen Steuergerät jedoch überführt wurde, den Schließmechanismus selbst durch vorschriftswidrige Nutzungen (zu hohe Geschwindigkeit bei Öffnung des Verdecks) beschädigt zu haben.[10]

Big Data im Fahrzeug wirft zugleich all jene Fragestellungen auf, die Datenschützer im Internet und insbesondere im Internet der Dinge bewegen. Gleichzeitig stellt das vernetzte Fahrzeug auch das Datenschutzrecht vor eine ganze Reihe neuartiger Fragestellungen, für die noch keine Antworten parat stehen. Das Bundesdatenschutzgesetz ist auf solche mehrpolaren Konstellationen nicht zugeschnitten. Hier sind sowohl der Gesetzgeber als auch die Aufsichtsbehörden gefordert, praktikable Lösungsansätze zu entwickeln und umzusetzen. Die 125 Jahre sozialer Erfahrung, die unsere Gesellschaft mit dem Automobil gesammelt hat, werden durch das vernetzte Kfz in Frage gestellt. Die datenschutzrechtliche Gretchenfrage lautet dann: Autonomes Fahren wird kommen – aber wird es dann noch so etwas wie „anonymes Fahren" geben?

Das vernetzte Auto ist – so mein erstes Resümee – kein Nebenschauplatz. Es wird im Zentrum des Internets der Dinge stehen, es ist das Paradebeispiel für die vernetzte Welt der Zukunft. Und die Forderung nach der Beachtung des informationellen Selbstbestimmungsrechts ist dabei kein juristisches Glasperlenspiel: „Es geht um einen Milliardenmarkt – und um einen massiven Angriff auf einen der letzten großen Räume der Privatsphäre und der Selbstbestimmung, der Millionen von Autofahrern unmittelbar betrifft."[11]

1 Das Geschäft mit den intimen Daten aus dem Auto, FAZ vom 28.01.2014.

2 Bentenrieder/Reiner/Wandres, Trends, Chancen und Lösungen für die Automobilindustrie, 2011.

3 http://www.businessinsider.com/ford-exec-gps-2014-1.

4 Schulzki-Haddouti, Schädliche Datenemission, c`t 2014, 62 ff.

5 Vgl. Herbert Braun, Wir sind auf dem Weg, Die Erforschung des autonomen Fahrens, c`t 2014, 136 ff.

6 Bundestags-Drucksache 18/1166.

7 Cichy, das vernetzte Fahrzeug – eine Bedrohung für die Privatsphäre?, PinG 2014, 200 ff.

8 Bundestags-Drucksache 18/1362, Seite 3.

9 Bundestags-Drucksache 18/1362, Seite 4.

10 c't 2014, 63.

11 Das Geschäft mit den intimen Daten aus dem Auto, FAZ vom 28.01.2014.

Frank Spaeing

PKW-Maut-Systeme in Europa

Wie die Diskussionen der letzten Monate in Deutschland zeigen, ist auch ein Maut-System eine Gelegenheit, viele Daten über Autofahrer zu sammeln. Der deutsche Vorschlag zur Infrastrukturabgabe (eine PKW-Maut darf es ja nach dem Willen der Kanzlerin nicht geben[1]) sieht nämlich durchaus einige Pflichten vor, personenbezogene und personenbeziehbare Daten zu verarbeiten. Weswegen die Deutsche Vereinigung für Datenschutz schon im letzten Jahr die Entwürfe des PKW-Maut-Gesetzes (Verzeihung, des Infrastrukturabgabengesetzes) kritisierte[2].

Ist es denn notwendig, die PKW-Maut so datenintensiv zu gestalten? Gibt es nicht Varianten, die deutlich datensparsamer daherkommen? Zeit, über den deutschen Tellerrand hinauszuschauen und zu betrachten, wie unsere europäischen Nachbarn mit diesem Thema umgehen. Der folgende Artikel bezieht viele Informationen aus der Zusammenstellung von europäischen Mautsystemen, die der Automobilclub von Deutschland (AvD) auf seiner Webseite[3] veröffentlicht hat. Wollen Sie demnächst mit Ihrem Kfz durch Europa fahren? Dann finden Sie dort umfassende Informationen zu Maut-Systemen in Europa.

Welche Maut-Systeme gibt es also in Europa?

Die Vignettenmaut – Die (meist) datensparsame Lösung

Als Erstes sind hier die Vignetten-Mautsysteme zu nennen. Bei diesen Systemen muss der Kfz-Besitzer auf der Frontscheibe (je nach Land gibt es hier unterschiedliche Regeln für die exakte Positionierung der Vignette) den Nachweis der gezahlten Maut, die Vignette, anbringen. Diese Vignetten sind so gestaltet, dass das Entfernen normalerweise nicht ohne Beschädigung der Vignette funktioniert. So soll das Ablösen und Weiternutzen von Vignetten an anderen Kfz verhindert werden.

Die Vignetten gibt es üblicherweise für verschiedene Zeiträume, angefangen bei 7-Tages-Vignetten bis zu Jahresvignetten.

Die Erfüllung der Mautpflicht wird also über ein optisch erkennbares Merkmal am Kfz nachgewiesen. Die Kontrolle erfolgt entweder über personalgestützte Kontrollen oder über optische Erfassung. Eine Vorab-Registrierung ist meist nicht notwendig; die Vignette kann an Tankstellen und anderen Verkaufsstellen bezogen und am Fahrzeug angebracht werden.



Mautstelle vor der Øresund Brücke

Natürlich können manche Vignetten über das Internet bezogen werden, eine Pflicht hierzu besteht aber üblicherweise nicht.

Diese Variante ist relativ datensparsam. Lediglich beim Bestellprozess im Internet werden üblicherweise personenbezogene Daten abgefragt. Auch ließe die Kontrolle durch Videokameras grundsätzlich die Erstellung von Bewegungsprofilen zu. Konkrete Hinweise dazu sind dem Autor allerdings nicht bekannt.

Länder, die (auch) die Vignetten-Maut nutzen sind: Bulgarien, Montenegro, Österreich (Fahrzeuge bis 3,5 Tonnen), Rumänien, Schweiz (Fahrzeuge bis 3,5 Tonnen), slowakische Republik, Slowenien und Tschechien.

Die Streckenmaut, ein in Europa häufig genutztes Mautsystem

Die zweite Variante, die in mehreren Ländern Europas anzutreffen ist, ist die Streckenmaut. Bestes Beispiel hierfür ist Dänemark. Dänemark hat grundsätzlich keine Kfz-Maut, einzige Ausnahme sind die Brückennutzungsgebühren für die Øresund Brücke und für die Storebaelt-Brücke. Jede Fahrt wird einzeln berechnet, die Gebühr richtet sich nach der Art des Kfz.

Weitere Länder, in denen es (auch) streckenabhängige Mautgebühren (meist für einzelne Tunnel und Brücken bzw. Autobahnteilstrecken, aber auch vereinzelt für das gesamte Autobahnnetz) gibt, sind: Frankreich, Griechenland, Großbritannien (zusätzlich auch Londoner Innenstadt-Maut, siehe unten), Italien (zusätzliche Stadt-Mautsysteme, siehe unten), Kroatien, Mazedonien, Montenegro (nur der Sozina-Tunnel), Norwegen, Österreich, Polen, Portugal (hier ist auch eine zeitliche Komponente enthalten, wer länger als 12 Stunden auf dem mautpflichtigen Streckenabschnitt ist, bezahlt die Mautgebühr mehrfach), Schweden, Schweiz, Serbien, Spanien (ohne kanarische Inseln) und die Türkei.

Wie werden die streckenabhängigen Mautgebühren erhoben?

Neben der Möglichkeit der Barzahlung, die bei fast allen genannten Systemen gegeben ist, wird oft auch Kartenzahlung angeboten oder die Nutzung von Maut-Zahlsystemen.

Diese können zum einen über Onboard-Units realisiert werden. In Frankreich zum Beispiel beim Maut-System „Liber-t"[4] wird jede Durchfahrt durch

eine Mautstelle durch die Onboard-Unit registriert und die Kosten dafür werden am Monatsende berechnet. In Österreich müssen Fahrzeuge über 3,5 Tonnen Gesamtgewicht die Go-Box nutzen. Diese kommuniziert mit an den mautpflichten Strecken angebrachten Sendern und ermittelt so die Mautgebühren. Diese können vorab aufgeladen oder nachträglich beglichen werden. Ein ähnliches System gibt es für alle Fahrzeuge in Serbien.

Zum anderen können auch einfache Chips oder Transponder im Fahrzeug angebracht werden. In Norwegen kann gegen Kaution ein Chip bezogen werden. Dieser wird vorab mit einem Geldbetrag aufgeladen und bei jeder Durchfahrt durch eine Mautstation wird der entsprechende Betrag berechnet. Wenn der Chip wieder zurückgegeben wird, werden der Restbetrag und die Kaution wieder ausgezahlt. Ob hier zentral zu jeden Fahrzeug die Nutzungsdaten erfasst werden oder nur zum Transponder die Bezahlinformationen, ist vom Autor nicht recherchiert worden.

An manchen Mautstationen in Norwegen gibt es keine Möglichkeit bar zu zahlen. Dort wird dann das Kfz-Kennzeichen fotografiert und man kann dann an den folgenden Tankstellen die Nutzungsgebühr entrichten. Allen Fahrzeughaltern, die nicht innerhalb von drei Tagen gezahlt haben, sendet die Mautgesellschaft (ohne Mehrkosten) eine Rechnung nach Hause.

Die Streckenmaut kann also zum einen ein sehr datensparsames Verfahren (anonyme Zahlung mit Bargeld an Mautstreckenposten) aber auch ein datenintensives Verfahren (Systeme mit Onboard-Units, die ggf. auch online angefragt werden) sein. Meist ist eine pragmatische Lösung bei Onboard-Units anzutreffen, diese können vorab aufgeladen (prepaid) und dieses Guthaben dann abgefahren werden.

Das volle Programm – die elektronische Mautgebühr

Vollelektronische Mautsysteme (ohne Transponder bzw. Vignette) gibt es momentan innerhalb Europas nur in Ungarn. Hier müssen sich Kfz-Nutzer über das Internet[5] zur sogenannten E-Vignette registrieren und E-Tickets beziehen. Dieses System ist am ehesten mit der in Deutschland geplanten Infrastrukturabgabe vergleichbar. Daten über Fahrzeughalter werden zentral gespeichert und stehen (u.a.) für Kontrollzwecke durch Behörden zur Verfügung. Wie auch in Deutschland diskutiert, sind dort für verschiedene Zeiträume E-Tickets beziehbar. Ob in Ungarn auch Bewegungsdaten erfasst werden, ist dem Autor nicht bekannt. In Deutschland waren diese zwischenzeitlich in Gesetzesentwürfen vorgesehen.

Wenn es richtig eng (und teuer) wird – die Stadtmaut

In manchen Städten sollen Mautsystem auch zum Steuern der Verkehrsdichte genutzt werden. So wird zum Beispiel in der Londoner Innenstadt für die „London Congestion Charge" pro Tag eine Gebühr von 11,50 Pfund fällig. Kontrolliert wird bei diesem System mittels automatischer Kennzeichenerfassung durch diverse in der Innenstadt verteilte Kameras. Die hierfür notwendigen Stammdaten des Fahrzeughalters müssen vorab auf einer Webseite bei der Registrierung des Kfz[6] erfasst werden. Meist sind diese Stadtmautverfahren eingeführt worden, um Staus in der Innenstadt zu verringern bzw. zu verhindern. In Norwegen wurde in manchen Städten die Stadtmaut eingeführt, um den Straßenausbau in der bergigen Region zu finanzieren. Nach Abschluss der Finanzierung wurde zum Beispiel in Trondheim 2005 die Stadtmaut wieder abgeschafft, nur um 2010 im Rahmen eines Umweltpakets wieder eingeführt zu werden.

Europäische Städte, in denen eine Stadtmaut erhoben wird, sind[7]: Durham und London (in Großbritannien), Mailand und Bologna[8] (in Italien), Valetta (in Malta), Bergen, Haugesund, Oslo, Kristiansand, Namsos und Trondheim (in Norwegen) und Stockholm und Göteborg (in Schweden).

Die Kontrolle der Mautzahlung erfolgt unterschiedlich. Von der Möglichkeit des Papiertickets (u.a. auch in Mailand) bis hin zur Vorab-Anmeldung über das Internet und der quasi lückenlosen Kameraüberwachung in London ist alles vertreten.

Europaweit wird in mehreren Städten schon länger über die Einführung einer City-Maut nachgedacht, weitere Informationen finden sich u.a. auf der dazugehörigen Wikipedia-Seite[9].

Fazit

Mautsysteme gibt es in Europa schon lange und immer häufiger. Nach Betrachtung der unterschiedlichen Umsetzung erscheint die deutsche Infrastrukturabgabe nicht als Ausreißer. Allerdings gibt es deutlich datensparsamere Varianten.

Wie technisch komplex oder arbeitsintensiv sind die diversen Mautsysteme? Da gibt es europaweit unterschiedliche Ansätze.

Bis auf Ungarn hat kein europäisches Land die Digitalisierung so weit vorangetrieben. Deutschland wäre erst das zweite europäische Land, das diesen komplexen Weg wählt.

Die EU-Kommission denkt derzeit über die Einführung einer europaweiten Maut nach[10]. Auch hier sollten schon bei der Konzeption des potenziellen Mautsystems die Prinzipien „Privacy by Design" und „Privacy by Default" berücksichtigt werden.

Datensparsame Mautsysteme sind möglich. Dies jedenfalls kann man festhalten. Und es wird in Zukunft sicherlich kein Weg an nationalen und vielleicht auch europaweiten Mautsystemen vorbei führen. Wichtig ist aber, dass der Datenschutz nicht auf dem Altar der vielfach fiskalisch und auch ökologisch motivierten Vorhaben geopfert wird.

1 http://zdfcheck.zdf.de/faktencheck/merkel-pkw-maut/.
2 https://www.datenschutzverein.de/wp-content/uploads/2014/11/2014_11-Maut.pdf.
3 https://www.avd.de/wissen/recht/verkehrsvorschriften-ausland/mautgebuehren-im-ausland/.
4 http://www.telepeagelibert.com/index.htm.
5 https://www.virpay.hu/de/autopalya-matrica-vasarlas.htm.
6 http://tfl.gov.uk/modes/driving/congestion-charge.
7 http://de.urbanaccessregulations.eu/.
8 http://www.comune.bologna.it/trasporti/servizi/2:4321/3246/.
9 https://de.wikipedia.org/wiki/Innenstadtmaut.
10 http://www.n-tv.de/ticker/EU-Kommissarin-Bulc-prueft-europaweite-Pkw-Maut-article14386001.html.

Thilo Weichert

Das Kfz, die Telematik und der Datenschutz


Bildquellen: ClipDealer.de | Frans Valenta

Die Automobilindustrie entwickelt sich zu einem Wirtschaftssektor, in dem es nicht nur um Mobilität geht. Insbesondere durch die Automation der Kraftfahrzeuge (Kfz) entstehen Schnittmengen und Ergänzungen. Die Techniken und Dienste dienen der Erhöhung der Sicherheit, der Reduzierung negativer Umwelteinflüsse, der Diagnose von Fahrzeugfehlern, dem Ruf nach Nothilfe, der Bekämpfung des Kfz-Diebstahls, der Navigationsunterstützung, der Bereitstellung von Information und Unterhaltung und vielem mehr.[1] Dabei bleiben die Informationen nicht im Kfz, sondern werden über Telematik mit externen Systemen verknüpft.

Die Perspektiven sind noch längst nicht ausgereizt: Es geht darum, den selbstfahrenden Personenkraftwagen (PKW) zu realisieren, bei dem sich der Fahrer anderen Fragen als der Verkehrssicherheit widmen kann. Beim automatisierten Verfahren von Lastkraftwagen (LKW) sollen auf Autobahnen ganze Züge elektronisch zusammengekoppelt werden, was nicht nur der effizienten Straßennutzung, sondern auch der effektiven Fahrernutzung, der Unfallsicherheit und der Umweltbilanz dienlich sein soll.[2] In den USA werden selbstfahrende Autos schon auf öffentlichen Straßen getestet.[3] Um insofern nicht abgehängt zu werden, haben Baden-Württemberg und Bayern angekündigt, die A81 und die A9 als Teststrecke für die fahrerlosen Autos der Zukunft freizugeben.[4] Auf der jährlich im Januar stattfindenden Consumer Electronics Show (CES) in Las Vegas wird jeweils der aktuelle technische Fortschritt präsentiert, wie sehr sich digitalisierte Autos in ihre Insassen „hineinfühlen“ und deren Wünsche realisieren können.[5]

Beteiligte

Ähnlich anderen arbeitsteiligen Prozessen in der Informationstechnik (IT) gibt es unterschiedliche Beteiligte. Im datenschutzrechtlichen Sinn betroffen ist vorrangig die FahrerIn, möglicherweise sind dies auch MitfahrerInnen. Diese müssen nicht identisch sein mit dem Halter, also dem Eigentümer, dem regelmäßig das Bestimmungsrecht über die Nutzung des Kfz zusteht. Halter muss keine Privatperson, kann auch der Arbeitgeber, ein Auto-Vermieter, eine Leasing-Geber oder ein Spediteur sein.

Für die Grundfunktionalität der Kfz-Datenverarbeitung verantwortlich ist der Kfz-Hersteller. Dieser wird regelmäßig ein umfassendes informationstechnisches Serviceangebot gemeinsam mit dem Auto bereitstellen. Er hat ein großes Interesse an den Nutzungsdaten für eine verbesserte Kundenbindung, aber auch zur langfristigen Qualitätssicherung und bedarfsgerechten Weiterentwicklung seiner Produkte. Eine wichtige Schnittstelle für den Hersteller und für andere Dienstleister sind die Werkstätten, bei denen im Rahmen von Wartung, Pflege und Reparatur weitere Daten anfallen. Die Werkstätten stöpseln ihre Geräte an die Diagnose-Schnittstelle eines Autos, OBD II genannt, und können Informationen über den Fahrzeugzustand abfragen, aber z. B. grds. auch, wann ein Auto schnell beschleunigt oder gebremst hat.[6]

Mit weiteren Dienstleistungen treten zusätzliche Akteure in Erscheinung: Hardware- und Softwareanbieter generell, etwa Browser-Hersteller, App-Anbieter, Betreiber von App-Marktplätzen, Versicherungen, Automobilclubs usw. Bei einer Online-Anbindung kommen Netzbetreiber bzw. Telekommunikationsanbieter hinzu. Google und Nvidia haben sich zu einer Open Automotive Alliance mit Audi, Honda, Hyundai und General Motors zusammengeschlossen. Auch Apple (mit Volvo, Ferrari) und Microsoft sind schon groß im Geschäft. Die Deutsche Telekom versucht hier, den Vertrauensbonus zu nutzen, den sie seit Edward Snowdens Enthüllungen als

europäisches Unternehmen genießt.[7] In einer Allianz, Genivi, mit Sitz im kalifornischen San Ramon haben sich Autohersteller, Zulieferer und Elektronikunternehmen zusammengeschlossen.[8]

Die bisher praktizierte Online-Kommunikation erfolgt regelmäßig zwischen Anbieter und Kfz, vermittelt durch Kfz-Hersteller und Telekommunikationsdienstleister. Eine Weiterentwicklung stellt die Car-2-Car-Kommunikation dar, bei der die Kfz sich untereinander und miteinander austauschen, etwa aus Sicherheitsgründen oder um bei Lastkraftwagen Kolonnen zusammenzuführen und zu lenken.[9]

Betroffene Grundrechte

Die Besonderheit der Kfz-Datenverarbeitung liegt darin, dass dabei regelmäßig Standortdaten erfasst werden[10], über die zu den Nutzenden Bewegungsprofile erstellt werden können, die zugleich aussagekräftig sind in Bezug auf Gewohnheiten, soziale Kontakte, Arbeit und Interessen. Zwischen Kfz und einer natürlichen Person besteht – zumeist intensiver als bei anderen Mobilgeräten – eine dauernde personale Verbindung; viele verbringen darin einen großen Teil ihres Tages. Oft erfolgt ein Austausch zwischen mobilem Auto und einer externen Infrastruktur.[11] Betroffen sind also die unterschiedlichsten persönlichen Lebensbereiche von Menschen.

Der Kfz-Automation ist ein hohes Überwachungsrisiko immanent. Werden digitale Daten im, am und über das Auto erfasst, so sind diese zur Kontrolle der FahrerIn, der Mitfahrenden oder des Halters in der Lage. Dabei kann in deren Recht auf informationelle Selbstbestimmung, in deren Grundrecht auf Datenschutz, eingegriffen werden.[12] Tangiert sein können auch weitere Ausprägungen des allgemeinen Persönlichkeitsrechts, etwa das Recht am eigenen Wort oder das am eigenen Bild oder, soweit es den engeren Bereich der persönlichen digitalen Sphäre betrifft, das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.[13] Weitere Grundrechte können berührt sein, etwa das Recht auf Mobilität als Ausprägung der allgemeinen Persönlichkeitsentfaltung, das Telekommunikationsgeheimnis des Art. 10 GG oder politische und ökonomische Grundrechte, wenn das Kfz in bestimmten Zusammenhängen zum Einsatz kommt. Aus diesen Grundrechten kann ein Anspruch auf spurenfreie Mobilität abgeleitet werden. Werden Informationen über die individuelle Kfz-Nutzung Dritten bekannt, so kann dies dazu führen, dass eine Person auf die Inanspruchnahme von grundrechtlich gesicherten Freiheiten verzichtet.[14]

Konkret erfolgt die Nutzung der Kfz-Daten schon heute bei der Aufklärung von Unfall-Geschehen. Die eigene Auto-IT wird zur Zeugin der Anklage, wenn Ermittlungsbehörden die Daten mit Hilfe eines richterlichen Durchsuchungsbeschlusses einfordern.[15] Ein solches Zeugnis können auch Versicherungen bei der Schadenbegleichung einfordern. Oder diese lassen sich die Daten über sog. „Telematik-Tarife" gleich ab Vertragsschluss frei Haus liefern.

Anwendbares Recht

Der IT-Einsatz im Auto unterscheidet sich bei Nutzung von Telematik kaum von sonstiger Mobilkommunikation. Das Kfz ist ein großes Smartphone auf Rädern mit vielen und einigen besonderen Applikationen bzw. Anwendungen. Gesonderte gesetzliche Regelungen gibt es – abgesehen von sehr spezifischen Anwendungen wie LKW- oder PKW-Maut, eCall u. Ä. – bisher praktisch nicht. Dies bedeutet, dass für die Verarbeitung von Inhaltsdaten das Bundesdatenschutzgesetz (BDSG), für die Verarbeitung von Nutzungs- und Bestandsdaten vorrangig das Telemediengesetz (TMG) und evtl. – in Bezug auf Netzbetreiber – das Telekommunikationsgesetz (TKG) anwendbar ist. Auf europäischer Ebene sind korrespondierend derzeit die europäische Datenschutzrichtlinie[16] und die Telekommunikations-Datenschutzrichtlinie[17] anwendbar.

Die rechtliche Legitimation von personenbeziehbarer Datenverarbeitung erfolgt regelmäßig per Vertrag, also insbesondere über Kauf-, Leasing- oder Mietvertrag, möglicherweise auch über den Vertrag mit einem Dienstanbieter auf Nutzung eines spezifischen Dienstes. Zulässig ist die Verarbeitung, die jeweils zur Erbringung des Dienstes erforderlich ist bzw. die im Vertrag ausdrücklich vereinbart wurde. Weitere Legitimationsgrundlage können berechtigte Interessen einer verantwortlichen Stelle sein, die mit den schutzwürdigen Betroffeneninteressen abzuwägen sind.[18] Die Datenverarbeitung kann weiterhin durch ein Spezialgesetz legitimiert sein, wobei es sich um ein Kfz-spezifisches Gesetz (z. B. LKW-Maut, eCall) oder um ein allgemeines Gesetz für einen spezifischen Zweck (z. B. Strafverfolgung: Strafprozessordnung, Unfallregulierung: BGB, ZPO) handeln kann. Schließlich ist eine Datenverarbeitung auf Einwilligungsbasis möglich.[19]

Öffentliche Diskussion

Die Diskussion über den Datenschutz im Straßenverkehr hat schon früh begonnen.[20] Eine größere Öffentlichkeit erreichte diese durch die Planungen zur Einführung einer LKW-Maut auf Autobahnen und die damit verbundene Erfassung des gesamten dortigen Verkehrs. Diese Debatte bekam durch die aktuellen Planungen der Bundesregierung neue Nahrung, auch für Personenkraftwagen (PKW) eine Maut einzuführen und dabei auf digitale Kontrollen zurückzugreifen.[21] Eine heftige verfassungsrechtliche Debatte erfolgte anlässlich der Einführung des anlasslosen Kfz-Kennzeichen-Scannings in vielen Landespolizeigesetzen, die ihren Höhepunkt fand, als das Bundesverfassungsgericht (BVerfG) die Regelungen von Hessen und Schleswig-Holstein als verfassungswidrig aufhob.[22] Einen explizit verbraucherrechtlichen Drive erhielt die Diskussion aber erst im Januar 2014, als sich öffentlichkeitswirksam der 52. Verkehrsgerichtstag in Goslar mit der Frage „Wem gehören die Fahrzeugdaten?" befasste und dabei folgende Positionen verabschiedete:[23]

1. Damit Innovationen für die Automobilität in Europa auch zukünftig gesellschaftlich akzeptiert werden, muss der Austausch von Daten und Informationen aus dem Fahrzeug Regeln unterworfen werden, die das informationelle Selbstbestimmungsrecht durch Transparenz und Wahlfreiheit der Betroffenen (z. B. Fahrzeughalter und Fahrer) sichern.

2. Fahrzeughersteller und weitere Dienstleister müssen Käufer bei Vertragsabschluss in dokumentierter Form

umfassend und verständlich informieren, welche Daten generiert und verarbeitet werden sowie welche Daten auf welchen Wegen und zu welchen Zwecken übermittelt werden. Änderungen dieser Inhalte sind rechtzeitig anzuzeigen. Fahrer sind geeignet im Fahrzeug zu informieren.

3. Bei der freiwilligen oder vertraglich vereinbarten Datenübermittlung an Dritte sind Fahrzeughalter und Fahrer technisch und rechtlich in die Lage zu versetzen, diese zu kontrollieren und ggf. zu unterbinden. Das Prinzip der Datensparsamkeit ist sicherzustellen. Für Unfalldatenspeicher, Event Data Recorder usw. ist ein Standard vorzuschreiben.

4. Bei Daten, die aufgrund gesetzlicher Regelungen erhoben, gespeichert oder übermittelt werden sollen, sind verfahrensrechtliche und technische Schutzvorkehrungen genau zu bestimmen.

5. Zugriffsrechte der Strafverfolgungsbehörden und Gerichte sind unter konsequenter Beachtung grundrechtlicher und strafprozessualer Schutzziele spezifisch zu regeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder richtete zu diesen Fragestellungen eine Arbeitsgruppe ein, die sich mit den vielfältigen mit der Digitalisierung des Autos und dessen multimedialer Vernetzung verbundenen Datenschutzfragen befasst. Am 08./09.10.2014 wurde von der Konferenz eine Entschließung mit folgendem Text verabschiedet:[24]

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer beziehungsweise den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikationsdiensten und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- *Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikationsdienste und Teledienste die Datenschutzgrundsätze von privacy by design beziehungsweise privacy by default zu verwirklichen.*
- *Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.*
- *Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.*
- *Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.*
- *Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und gegebenenfalls zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.*
- *Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und Datenintegrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.*

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

Die internationale Dimension – die USA

Die Debatte um den Kfz-Datenschutz hat inzwischen die Kfz-Hersteller erreicht. Dies gilt nicht nur für den europäischen, sondern auch für den US-amerikanischen Markt. Einer der Hintergründe ist, dass die Produktion von Kfz für einen ausschließlich nationalen oder regionalen Markt kostenträchtig ist und deshalb vermieden werden soll. Bedürfnisse nach Privatheit bestehen nicht nur in Europa, sondern weltweit. Andererseits zeigt die Internetwirtschaft, welchen ökonomischen Wert personenbeziehbare Daten aus dem Konsumentenalltag darstellen können und welche globalen Marktpotenziale sich hieraus ergeben. Diese Potenziale möchten nicht nur die Kfz-Hersteller entfalten, sondern allen anderen Branchen voran auch die bisherige Internet- und IT-Wirtschaft. Es kommt nicht von ungefähr, dass sich die großen IT-Unternehmen massiv in diesem Bereich engagieren und dabei sogar teilweise – ohne Kooperationen mit Kfz-Herstellern – auf eigene Lösungen setzen.

In diesem Wettbewerb zwischen IT- und Kfz-Industrie verfolgen interessanterweise global die Kfz-Hersteller ein gemeinsames Interesse an einem gewissen Datenschutz, mit dem sie sich von der IT-Wirtschaft abzusetzen versuchen,

für deren Silicon-Valley-Kapitalismus es keine durch Privatheitsbedürfnisse oder Datenschutzgesetze eingegrenzte wirksamen Beschränkungen zu geben scheint. Insofern ist es nicht erstaunlich, dass die Hersteller für den US-amerikanischen Markt sich konzern- und herkunftsunabhängig im November 2014 in der Alliance of Automobile Manufacturers (AAM) und der Association of Global Automakers (AGA) über „Consumer Privacy Protection Principles – Privacy Principles for Vehicle Technologies and Services“ verständigt haben.[25] Zu der Allianz gehören US-Firmen (Chrysler, Ford, General Motors) ebenso wie deutsche (BMW, Mercedes-Benz, Porsche, VW) und sonstige europäische (Aston Martin Lagonda, Ferrari, Maserati, Volvo) sowie asiatische Unternehmen (Honda, Hyundai, Kia, Mazda, Mitsubishi, Nissan, Subaru, Toyota).

In diesen US-amerikanischen Privacy-Grundsätzen werden keine klaren, normativen Festlegungen vorgenommen, sondern Ziele in sehr allgemeiner Form beschrieben .Es handelt sich um folgende Ziele: Transparenz, Wahlmöglichkeit, Kontextangemessenheit, Datenminimierung (inkl. De-Identifikation und Speicherdauer), Datensicherheit, Integrität & Auskunft, Verantwortlichkeit.[26] Die Ziele werden regelmäßig nicht umfassend, sondern nur in „vernünftiger Form“[27] angestrebt. Die Bestimmungsmacht liegt gemäß den „Principles“ unzweifelhaft beim Hersteller, nicht beim Betroffenen. Als besonders sensibel werden angesehen: Standortdaten, biometrische Informationen und Angaben über das Fahrverhalten. Insofern sollen klare und aussagekräftige Angaben bzgl. Zweckbestimmung und verantwortliche Stellen gegeben werden. Die Nutzung eines Dienstes nach vorangegangener Information wird als Einwilligung interpretiert. Bei den sensiblen Daten wird eine explizite Einwilligung zugestanden, von der es aber wieder Ausnahmen gibt, z. B. für Zwecke der Sicherheit, der Eigenforschung, der Produktentwicklung oder auch zur Einschaltung von Dienstleistern. Hinsichtlich der Zweckfestlegung genügt eine Information, die auch weitläufig oder allgemein sein kann. Keine Zweckbeschränkung ist bzgl. eines großen Ausnahmekatalogs vorgesehen, in dem die Forschung, die Produktverbesserung und auch die Werbung aufgeführt werden. Auch Integrität (Berichtigung) und Auskunft werden nur gewährt, soweit dies vernünftig („reasonable“) ist.

Diese Grundsätze sind zweifellos besser als nichts. Da sie aber unverbindlich und offen formuliert sind und keine Implementierungs-, Kontroll- oder Beschwerdemaßnahmen vorsehen, tendieren sie eher zu einem Werbeversprechen; datenschutzrechtliche Zusicherungen sind sie nicht.

Die VDA-Prinzipien

Fast zeitgleich zu den US-Grundsätzen der AAM/AGA veröffentlichte der deutsche Verband der Automobilindustrie (VDA) mit Datum vom 03.11.2014 „Datenschutzprinzipien für vernetzte Fahrzeuge“.[28] Werden die beiden Dokumente nebeneinandergehalten, so verblüfft deren Ähnlichkeiten bei Aufbau und Inhalt. Es gibt aber wesentliche Unterschiede. So bekennen sich die Hersteller und Zulieferer im VDA bei Entwicklung und Betrieb der IT zu den Grundsätzen des „privacy by design“. Bei Unternehmenskooperationen wird die Information „an den entsprechenden Schnittstellen“ zugesagt, „wer Diensteanbieter und ggfs. Vertragspartner ist“. Die Kategorisierung der Daten ist differenzierter als in den USA und eskaliert von „erzeugten technischen Daten“ bis zu „Daten aufgrund gesetzlicher Regelung“, wobei technischen Daten auf einer „Landkarte“ keine bzw. nur eine geringe Datenschutzrelevanz zugemessen wird, die „soweit möglich“ im Fahrzeug bleiben sollten und bzgl. der „ein überwiegendes berechtigtes Interesse … bezogen auf Fahrzeug- und Produktsicherheit bestehen“ könne. Erst eine „Kombination von Daten“ würde zur „Datenschutzrelevanz“ führen. Die VDA-Mitglieder setzen sich dafür ein, „dass für die Soft- und Hardwarearchitekturen der Fahrzeuge sowie Remote-Zugriffe auf das Fahrzeug über die Telekommunikation Standards etabliert und fortentwickelt werden, die ein hohes technisches Sicherheitsniveau fortlaufend gewährleisten.“[29]

Die VDA-Prinzipien sind kürzer als die der AAM/AGA, was dem Umstand zuzuschreiben sein dürfte, dass anstelle der in den USA statuierten Ziele in Deutschland gesetzlich verbindliche Ansprüche bestehen. Umso wünschenswerter wäre es gewesen, dass deren Umsetzung konkretisiert wird. Die Prinzipien können allenfalls ein allererstes Ergebnis einer herstellerinternen Verständigung sein. Doch ähnlich wie in den USA scheint diese Verständigung weniger darauf gerichtet zu sein, die Verbraucherrechte zu stärken, als darauf, die Definitionshoheit über die Datenverarbeitung zu bewahren .

So ist zu erwarten, dass über die angestrebten gemeinsamen Standards einheitliche Schnittstellen der Kfz-IT zu herstellerbeherrschten Verteilrechnern festgelegt werden.[30] Dies mag im Interesse der Datensicherheit sinnvoll sein. Zugleich wahren die Hersteller so die Kontrolle über die weitere Verteilung der Daten und können z. B. festlegen, zu welchen Werkstätten oder sonstigen Dienstleistern automatisiert Kontakte aufgenommen oder zumindest angeboten werden. Dieses Interesse steht im Widerspruch zu alternativen Anbietern von Kfz-nahen Dienstleistungen, etwa aus dem Bereich der Versicherungen oder dem der Automobilclubs. Es gibt gegenläufige Interessen etwa der Hersteller und der Kfz-Versicherer bei Unfällen, welche Werkstätte der FahrerIn bevorzugt angeboten wird. Heute bestehen schon bei Verträgen mit Herstellern, Versicherungen oder Automobilclubs oft Koppelungen[31], die für den Kfz-Halter bedeuten können, dass er sich bei vertragskonformem Verhalten gegenüber einem Vertragspartner gegenüber einem anderen zwangsläufig vertragswidrig verhält. Insofern ist zu erwägen, ob nicht im Interesse der VerbraucherInnen explizite Koppelungsverbote vorgesehen werden müssen.

eCall

Ab April 2018 sollen alle neuen Personenkraftwagen und leichten Nutzfahrzeuge in der EU verpflichtend mit „eCall“ ausgestattet werden, ein in der Kfz-Elektronik installiertes Verfahren, mit dem automatisch oder manuell bei einem Unfall, z. B. bei Auslösen des Airbags oder einer Panne, ein Notruf an die Nummer 112 ausgelöst wird.[32] Dies soll über eine voreingestellte mobile Datenübertragung inklusive Standortdatum an die nächste Rettungsleitstelle erfolgen. Automatisch soll eine Ton-

verbindung aufgebaut werden, um eine Kommunikation zwischen Rettungsleitstelle und Insassen zu ermöglichen. Die EU-Kommission erhofft sich mit diesem System wegen der dadurch ermöglichten schnelleren adäquaten Hilfe eine Senkung der Zahl der Unfalltoten um bis zu 2.500 im Jahr. Im Juni 2013 gab die EU-Kommission bekannt, dass sie EU-weit einheitliche technische Standards festgelegt hat. Das EU-Parlament wollte das Verordnungspaket im März 2015 absegnen.

Die Regelungen zielen auf Transparenz für die Betroffenen, Datensparsamkeit und Zweckbindung der verarbeiteten Daten ab. Offen ist noch die konkrete technisch-organisatorische Umsetzung. Zugleich sieht die Verordnung vor, dass es den Fahrzeugherstellern und unabhängigen Anbietern unbenommen bleiben soll, die dann installierte Technik für zusätzliche Notfalldienste und „Dienste mit Zusatznutzen" zu verwenden. Es geht den EU-Gremien nicht nur um ein zusätzliches Instrument der Verkehrssicherheit, sondern auch darum, in der Kfz-IT zunächst für diesen Dienst einheitliche Standards einzuführen und zugleich eine technische Plattform für eine weitergehende Informatisierung des Autos zu schaffen.

Die bordeigene Mobilfunkeinheit soll nur dann Verbindung zum Netz aufnehmen, wenn tatsächlich ein Notfallruf abgesetzt wird. Ein dauerndes „Tracking" mit der Bildung eines genauen Bewegungsbildes, wie es heute z. B. mit eingeschalteten Handys möglich ist, findet bei eCall nicht statt. Die FahrerIn kann aber das System nicht abschalten. Dies wird damit gerechtfertigt, dass es beim eCall nicht nur um den Schutz der FahrerIn, sondern auch von weiteren Verkehrsbeteiligten geht. Dies hat zwangsläufig in der lange dauernden Einführungsphase eine informationelle Ungleichbehandlung von Fahrten mit neuen und alten noch nicht mit eCall ausgestatteten Autos zur Folge. Es ist fraglich, ob das angestrebte Ziel diese Einschränkung der informationellen Selbstbestimmung rechtfertigen kann.[33]

PKW-Maut

Das Bundesverkehrsministerium stellte im Oktober 2014 einen Entwurf für ein PKW-Maut-Gesetz vor, wonach HalterInnen von PKW eine Infrastrukturabgabe (Maut) entrichten müssen, wenn sie Autobahnen und Bundesstraßen nutzen. Halter von im Inland zugelassenen PKW sollen die Abgabe vorab beim Kraftfahrtbundesamt (KBA) per Lastschrift entrichten, wozu dort in einem Infrastrukturabgaberegister Informationen zum PKW, zur Kontobeziehung sowie zur Entrichtung der Abgabe gespeichert werden sollen. Halter ausländischer PKW sollen Zeitvignetten erwerben können. Die Überwachung der Einhaltung der Abgabenpflicht obliegt dem Bundesamt für Güterverkehr (BAG). Hierzu sollten zunächst folgende Daten erhoben und weiterverarbeitet werden: Bild des Kfz, Name und Anschrift des Kfz-Führers, Ort und Zeit der Kfz-Nutzung, Kfz-Kennzeichen und abgaberelevante Kfz-Merkmale. Über eine mindestens 13 Monate dauernde Speicherung beim BAG sollte der Nachweis einer Nichtnutzung der Straßen zum Zweck der Rückerstattung der voraus bezahlten Abgabe ermöglicht werden. Der Entwurf enthielt zwar eine strenge Zweckbindung der Daten, hätte aber dazu geführt, dass zwecks möglicher Rückerstattung von wohl weniger als 1% der tatsächlich erfolgten inländischen Mautzahlungen beim BAG sämtliche über PKW-Maut-Kontrollstellen erfassten Kfz-Bewegungen mit Ort, Zeit und Foto von 100% aller PKWs über ein Jahr lang elektronisch gespeichert worden wären. Trotz versprochener Zweckbindung forderten Polizeivertreter schon Zugriff auf die künftige Datenbank. Eine derartige Vorratsspeicherung sämtlicher PKW-Bewegungen in Deutschland wurde von den Datenschutzbeauftragten unisono heftig kritisiert.[34]

Der im Dezember 2014 vom Bundeskabinett beschlossene Gesetzentwurf (BR-Drs. 648/14) sieht keine Bewegungsdatenbank beim BAG mehr vor. Inländer sollen ihren Nachweis für den Rückzahlungsanspruch und für das Nichtnutzen von Bundesstraßen selbst erbringen und „glaubhaft" machen, etwa durch ein Fahrtenbuch. Die umfassende zentrale Fahrtdatenspeicherung wird ersetzt durch individuelle Nachweissammlungen. Nachweiskonflikte im Fall von Rückforderungen sind vorhersehbar. Unabhängig davon wird dennoch eine umfassende Kontrolle des gesamten PKW-Verkehrs mit einem Abgleich des Registers der zahlenden PKWs zugelassen. Auf das beim KBA geführte Register mit Zahlungsangaben will der Entwurf also ebenso nicht verzichten wie auf die elektronische Überwachung der Mautzahlung. Der Entwurf behauptet fälschlich, damit „datensparsam" vorzugehen. Datensparsam wäre, wenn auf die Umsetzung der PKW-Maut völlig verzichtet würde oder man sich andere EU-Staaten zum Vorbild nähme, die mit einer Plakette und nicht mit Daten Mautgebühren erheben (siehe vorstehenden Artikel zu PKW-Maut-Systemen in Europa).

Kfz-Kennzeichen-Scanning

Kfz-Kennzeichen-Scanning hat in Deutschland schon eine wechselvolle Geschichte hinter sich. Es wurde bei der LKW-Maut-Einführung heftig diskutiert und konnte schließlich nur durchgesetzt werden, nachdem der Gesetzgeber in das Gesetz eine strenge Zweckbindung hineingeschrieben hatte.[35] Dieser Technik wurde eine „rote Karte" ausgestellt, als deren anlasslose Nutzung für die polizeiliche Gefahrenabwehr vom Bundesverfassungsgericht 2008 massiv eingeschränkt und Regelungen aus Hessen und Schleswig-Holstein als verfassungswidrig aufgehoben wurden.[36] Das Bundesverwaltungsgericht bestätigte in einer fragwürdigen Entscheidung die Rechtmäßigkeit der bayerischen Regelung;[37] hierzu ist eine erneute Beschwerde beim Bundesverfassungsgericht anhängig.[38]

In Niedersachsen soll in Kürze erstmals – ohne gesetzliche Grundlage – die Geschwindigkeitskontrolle auf der Basis des Kfz-Kennzeichen-Scannings über eine längere Fahrstrecke realisiert werden (sog. Section Control). Vergleichbare Planungen bestehen in anderen Bundesländern. Bei der Section Control erfolgt zunächst eine Erfassung von Kennzeichen, Ort und Zeit; dieser Datensatz wird nach einer festgelegten Strecke mit den dort erneut erfassten Daten abgeglichen. Selbst bei einer Pseudonymisierung der Eingangsdaten erfolgt somit eine zumindest kurzfristige Datenspeicherung. Für diese und die dann anschließenden Verarbeitungsschritte gibt es derzeit keine valide

Rechtsgrundlage. Deshalb bedarf es vor – auch testweiser – Einführung von Section Control einer expliziten klaren, verhältnismäßigen gesetzlichen Grundlage.

Was viele AutofahrerInnen nicht ahnen, ist, dass Kfz-Kennzeichen-Scanning im privaten Bereich bei Parkhäusern, Campingplätzen und Waschanlagen schon weit verbreitet ist. Ein einziger Hersteller in diesem Markt gab im Oktober 2014 an, allein im laufenden Jahr bereits 200 Parkhäuser und Parkplätze ausgerüstet zu haben. Zweck der Erfassung sind Abgleiche mit „Whitelists“ und/oder „Blacklists“, um Zufahrtsbefugnisse zu überprüfen. Aber auch andere Zwecke werden mit dieser hocheffizienten und inzwischen preiswerten Technik verfolgt, etwa „Marketingerfolgskontrolle“. Rechtlich legitimiert sind derartige heimliche Erfassungen in keinem Fall. Im privaten Bereich bedarf es hierfür entweder der ausdrücklichen Einwilligung oder einer ebenso expliziten vertraglichen Absprache.[39]

Ausblick

Weitere um sich greifende IT-Anwendungen im Kfz sind Versicherungstarife, die für defensives Fahren einen Bonus einräumen[40], sog. Dashcams[41], „intelligente Systeme“ der Stromversorgung im Bereich der Elektromobilität[42], Carsharing-Projekte und Mitfahrdienste wie das umstrittene Uber[43]. In jedem Fall werden umfangreich personenbezogene Daten erfasst und weiterverarbeitet.

Der Vormarsch der Kfz-Automation ist nicht aufzuhalten. Wer völlig ohne digitale Spuren unterwegs sein möchte, muss auf sein Auto verzichten. Selbst der Oldtimer wird zum Objekt des Kfz-Kennzeichen-Scannings. Informationstechnik im, am und um das Auto kann nützlich sein. Es kann deshalb nicht um deren Verhinderung, sondern muss um deren richtige Gestaltung gehen. Wichtig ist, dass das Prinzip der Datensparsamkeit bei allen Anwendungen berücksichtigt wird[44] und dass den Betroffenen auf eine verständliche und wahrnehmungsfähige Weise Transparenz vermittelt wird[45] sowie Wahlmöglichkeiten eingeräumt werden.[46] Das „Hacking“ von Autos muss durch technische Vorkehrungen so gut wie unmöglich gemacht werden – egal ob der Angriff von Kriminellen oder vom Staat kommt.[47]

Rechtlich sind nur in ausgewählten Bereichen Sonderregelungen für den Kfz-Datenschutz sowie für sonstige neu mit der Kfz-Automation auftretende Rechtsfragen nötig und sinnvoll.[48] Valide, allgemeine Datenschutzregelungen für mobile vernetzte Geräte würden die wesentlichen Ziele des Schutzes informationeller Selbstbestimmung und sonstiger Verbraucherrechte auch beim Kfz gewährleisten. Dies gilt für Forderungen nach Privacy by Default und Privacy by Design, für die Herstellung von Transparenz, die Garantie der Betroffenenrechte, für eine Präzisierung von Einwilligungserfordernissen oder für Koppelungsverbote.[49]

Konkretisierungen der rechtlichen Vorgaben können von der Kfz-Wirtschaft sowie von weiteren Sektoren in Kooperation mit den Datenschutzaufsichtsbehörden in Verhaltensregeln nach § 38a BDSG selbst vorgenommen werden. Eine solche Vorgehensweise wäre schneller und problemadäquater als zu spezifische Gesetzgebung. Steigt das Bewusstsein bei Bevölkerung, Medien und Politik in diesem Bereich, kann auch der nötige öffentliche Druck generiert werden, um die Bereitschaft zum Verhandeln solcher Verhaltensregeln zu schaffen. Durch Standardisierungen und einheitliche Schnittstellen-Festlegungen sollten ein hohes Sicherheitsniveau und die Gewährleistung der Betroffenenrechte garantiert und Koppelungszwänge verhindert werden. Ein geeignetes Instrument zur Gewährleistung hoher Datenschutzstandards können auch Zertifizierungen, Gütesiegel und Auditverfahren sein.

Die Diskussion um den Kfz-Datenschutz darf sich nicht ausschließlich auf das Auto selbst konzentrieren. Durch neue Praktiken der Verkehrs- und Parkraumlenkung, der Mauterhebung und der Verkehrsorganisation generell entstehen immer mehr analoge und digitale Schnittstellen zwischen Kfz und Umwelt, die bei einem umfassenden Datenschutzkonzept unserer Gesellschaft im Hinblick auf Mobilität mit berücksichtigt werden müssen. Zunehmen werden weiterhin die Begehrlichkeiten Dritter, nicht nur von Polizei und Versicherungen. Die Liste potenzieller öffentlicher wie privater Bedarfsträger scheint grenzenlos und geht von Geheimdiensten über die Finanzämter bis zu den Kommunen, von den großen IT-Anbietern über Arbeitgeber und Dienstleister bis zur Werbewirtschaft.

1 Stephan, Computer auf Rädern, SZ 31.01./01.02.2015, 64; Fromme, Sie haben Ihr Ziel erreicht, SZ 16,06.2014, 3; Alliance of Automobile Manufacturers, Inc./Association of Global Automakers Inc. – AAM/AGA, Consumer Privacy Protection Principles, Privacy Principles, Privacy Principles for Vehicle Technologies and Services, November 12, 2014, S. 1 (Fn. 25).

2 Eiger, Auf den Straßen surfen, Der Spiegel 22/2014, 108 f.; Wüst, Geisterbahn der Güter, Der Spiegel 28/2014, 115.

3 Fromm/Kuhn, Alles auf Autopilot, Die Geisterfahrer, SZ 13./14.09.2014, 30.

4 Fromm, Roboter an Bord, SZ 28.01.2015, 17.

5 Becker, Die Neuvermessung der Welt, SZ 10./11.01.2015, 72.

6 Bernau/Fromm/Maier/Martin-Jung, Der gläserne Autofahrer, SZ 28.01.2015, 20.

7 Bernau/Fromm, Digitale Durchstarter, SZ 10.10.2014, 17.

8 Martin-Jung, Das rollende Smartphone, SZ 12.09.2014, 20.

9 Dazu Bönninger (Fn. 23), S. 234 f.; Weichert SVR 2014, 202 = Fn. 23, S. 288.

10 Rechtlich dazu ausführlich Weichert, Datenschutz im Auto, SVR, 206 f.

11 Rechtlich zur Profilbildung Weichert SVR 2014, 241 f.

12 Art. 8 EuGRCh, BVerfG NJW 1984, 419.

13 BVerfG NJW 2008, 822.

14 Weichert, SVR 2014, 203 m. w.

15 Mielchen (Fn. 23), S. 245 ff.

16 95/46/EG; künftig die Europäische Datenschutz-Grundverordnung.

17 2002/58/EG.

18 Z. B. § 28 Abs. 1 S. 1 Nr. 2 BDSG.

19 §§ 4 Abs. 1, 4a BDSG, § 13 Abs. 2 TMG.

20 Zu den Anfängen Weichert, Anforderungen des Datenschutzes an den „intelligenten Straßenverkehr“, DuD 1996, 77.

21 DatenschützerInnen warnen vor PKW-Maut-System, DANA 2/2014, 168.

22 BVerfGE 120, 378 = NJW 2008, 1505.

23 Sämtliche Vorträge sowie Beschlussfassungen: 52. Deutscher Verkehrsgerichts-

tag 2014, 2014, S. XV, mit Beiträgen von Bönniger, S. 229, Mielchen, S. 241, Roßnagel, S. 257, Weichert, S. 285 (= SVR 2014, 201, 241).

24 Nachweis z. B. http://www.datenschutz.sachsen-anhalt.de/konferenzen/nationale-datenschutzkonferenz/entschliessungen/entschliessungen-der-88-datenschutzkonferenz-8-9-oktober-2014-in-hamburg/datenschutz-im-kraftfahrzeug-automobilindustrie-ist-gefordert/.

25 Nachweis: http://goodtimesweb.org/industrial-policy/2014/ConsumerPrivacyPrinciplesforVehicleTechnologiesServicesFINAL.pdf, vgl. Fn. 1.

26 Transparency, Choice, Respect of Context, Data Minimization, De-Identification&Retention, Integrity&Access, Accountability.

27 Reasonable steps.

28 Schulzki-Haddouti, Datenschutz im Auto, www.heise.de 22.12.2014; Nachweis: https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html.

29 Einen Überblick über die bisherige Praxis von Audi, BMW und Daimler gibt Schulzki-Haddouti, Autokonzerne interpretieren Datenschutz unterschiedlich, VDI-Nachrichten, 13.06.2014, 4.

30 Fromm, Interview mit Stadler, „Die Hoheit im Auto hat allein der Hersteller“, SZ 04.12.2014, 25.

31 Fromme, Kundenbindung, SZ 17.10.2014, 24.

32 Krempl, Grünes Licht im EU-Rat für Auto-Notruf eCall, www.heise.de 10.12.2014.

33 Weichert, SVR 2014, 245.

34 Nachweis: https://www.datenschutz-hamburg.de/uploads/media/Entschliessung_DSK_PKW-Maut.pdf; Deutsche Vereinigung für Datenschutz, DANA 4/2014, 167; DANA 4/2014, 168 f.

35 § 7 Abs. 2 S. 2 Autobahnmautgesetz.

36 BVerfGE 120, 378 = NJW 2008, 1505.

37 BVerwG, U. v. 22.10.2014, 6 C 7.13, DANA 4/2014, 183 f.

38 Kauß, Die präventive Kontrolle des öffentlichen Raumes durch die automatische Kfz-Kennzeichenerfassung, DuD 2014, 627.

39 Baars/Brühl/Deker, Wir wissen, wo du gestern geparkt hast, SZ 22.10.2014, 27.

40 „Pay as you drive“ bei Signal Iduna, DANA 4/2014, 17

41 Weichert SVR 2014, 246, AG München B. v. 13.08.2014, Az. 345 C 5551/14; VG Ansbach, U. v. 12.08.2014, AN 4 K 13.01634; DANA 3/2014, 134.

42 Klein/Mayer, Elektromobilität & Datenschutz, Neue Mobilität 10, Januar 2013, 52f; http://www.bem-ev.de/elektromobilitat-datenschutz/.

43 Heidtmann, Moderne Räuber, SZ 26./27.07.2014, 2.

44 Dazu präziser Weichert SVR 2014, 205 f.

45 Rechtlich dazu Weichert SVR 2014, 242 f., 244.

46 Weichert SVR 2014, 243 f.

47 Martin-Jung, Die Auto-Hacker, SZ 24.07.2014, 18; Hägler, Lasst uns endlich Daten sehen, SZ 06./07.12.2014, 2; Weichert SVR 2014, 244 f.

48 Stephan, Neuland, SZ 31.01./01.02.2015, 64.

49 Weichert SVR 2014, 246 f.

Snoopy

Roboter auf Rädern – eine leise Polemik wider den Markt

Zum Autor: Snoopy ist seit dem Studium in London ab ca. 1980 in der IT tätig. Damals hieß das noch EDV oder gar Mittlere Datentechnik[1] und war recht teuer. Ein paar Kostenrevolutionen später haben nun Menschen Zugang zu hoher Rechenleistung, die das, ehrlich gesagt, lieber bleiben lassen sollten. Snoopy turnt seit ca. 20 Jahren als Selbstständiger durch diverse Kundennetze und ist verwundert über die Leidensfähigkeit des Menschen, mit derartig verbogener Infrastruktur etwas hinzubekommen, was nur vage an produktive Arbeit erinnert. Seine verstorbene Mutter hat nie gewusst, dass er in so einem dreckigen Geschäft wie IT-Security ist; sie dachte immer er wäre Pianist im Edelbordell.

Wie die launige Vorstellung impliziert, handelt es sich bei dieser Polemik allein um die Meinung des Autors und nicht etwa um die der Deutschen Vereinigung für Datenschutz. Es ist eine satirische Glosse, obwohl die Tatsachen durchaus stimmen.

Der obige Titel dieser Polemik ist natürlich angelehnt an den Spruch der „Höhlenmenschen auf Rädern“, wobei heutzutage diese Höhlenmenschen immer mehr durch Roboter oder sogenannte „rechnergestützte Systeme“ ersetzt oder entmündigt werden.

Aktueller Anlass ist auch eine Meldung, welche kürzlich durch die Presse ging: BMW Fahrzeuge waren sehr einfach angreifbar, weil die Internet-Anbindung, das sogenannte BMW-Connect, der Kfz über normales HTTP-Protokoll lief und nicht etwa mit Hilfe des „sicheren“ HTTPS-Protokoll[2] realisiert wurde.

Natürlich wurde die Meldung platziert, als BMW nach eigenen Angaben die Lücke schon geschlossen hatte. Warum trau ich dem Braten nicht?

Erinnern wir uns kurz, dass BMW vor ein paar Jahren großflächig damit warb, dass ein BMW der Oberklasse mehr Rechenleistung auf die Straße bringt, als das gesamte Apollo-Mondlandeprogramm der NASA (einige Leser erinnern sich sicher noch daran).

Der Ansatz an sich ist ja gar nicht so blöd, es ist eigentlich relativ einfach, wenn auch ein wenig kostenintensiv, einen Roboter auf den Mond[3] oder gar Mars[4] oder vorbeifliegende Kometen[5] etc.[6] zu schicken und dort recht produktiv arbeiten zu lassen. Wurde auch schon von mehreren Ländern erfolgreich gemacht.

Einen Roboter zu bauen, der es alleine über eine viel befahrene Straße schafft, ist bis dato aber noch nicht einmal BMW gelungen und hier liegt ein Nagetier im exotischen Gewürz: Straßen sind hochdynamische und komplexe Systeme, welche für kybernetische Autarkie denkbar schlecht geeignet sind. Straßen sind kein Schachbrett und spielen auch kein Nullsummen-Spiel. Wie geübte Fernsehkrimi-Zuschauer wissen, geht ein Auto sofort in Flammen auf, sobald es die geteerte Fahrbahn verlässt, das ist serienmäßig ohne Aufpreis bei jedem Auto so. Straßen sind brandgefährlich.

Umso mehr beunruhigen mich die Ansätze der Kfz-Industrie, die da immer mehr Systeme in Autos einbauen, welche den Fahrer beobachten, entmündigen und letztlich überflüssig machen sollen.

Rollenwechsel

Interessant ist ein Aspekt, nämlich der schleichende Rollentausch zwischen Fahrer und Fahrzeug. Früher, zu meiner Zeit, beobachtete der Fahrer den Zustand des Kfz und seine (oder ihre) Einschätzung über die angezeigten Zustände wie Öldruck, Batterie, Tankfüllstand etc. entschied darüber, ob eine Fahrt angetreten wurde oder nicht.

Heute fährt das Auto nicht nur die Passagiere umher, sondern erstellt auch diverse Diagnosen, welche dem Bordrechner Aufschluss über das Fahrzeug geben. Wenn der Rechner aufgrund dieser Daten der Meinung ist, das Kfz ist nicht fahrtauglich, dann bewegt sich der Wagen nicht.

Der Fahrer selbst wird auch immer mehr beobachtet durch Müdigkeits-Assistenten (als ob man als dauergestresster Bürohengst überhaupt einen Assistenten braucht um müde zu werden!) und Spurhalte-Systeme etc. Wie oft und bei welchem Fahrer (Achtung: Datenfalle durch die Zuordnung des Fahrerprofils) diese dann ansprechen wird auf lange Zeit in einem Black-Box-Fahrtenschreiber gespeichert. Dieser kann und vor allen Dingen **wird** ggf. per Gerichtsbeschluss beweiskräftig ausgewertet[7].

So ergibt sich zum Beispiel durch Messung des Zeitraums zwischen Betätigung des Bremspedals und der Zündung des Airbags (also dem Zeitpunkt der Kollision), ob der Fahrer seine Schreck-Sekunde als Einladung zum Büroschlaf gewertet hat oder gar rechtzeitig reagiert hat. Ebenso wird registriert, ob der Blinker gesetzt war, wie lange vor der Kollision etc. Das Fahrverhalten des Fahrers wird feingranular protokolliert und gespeichert. Keine Fummelei am Autoradio oder Mitfahrern geschieht mehr ohne Beobachtung.

Andere rechtliche Fragen tun sich auf: Was ist, wenn die Autoversicherungen diese Daten auswerten dürfen, anonymisiert, räusper, räusper, natürlich. In meiner Praxis habe ich aber oft erlebt, dass angeblich anonymisierte Daten eigentlich normale Produktiv-Daten waren. Solange die Auswerter glauben, dass sie anonym sind, ist das doch alles gut. Honi soit, qui mal y pense[8].

Was tun bei Leihwagen? Ich habe einen Unfall und das Protokoll der Black-Box weist mich als vollkommenen Straßen-Rowdy aus, dabei war das der Fahrstil des Vormieters. Ein ähnliches Problem ergibt sich beim Verkauf eines Autos.

Angenommen, ich war oder bin krank, nehme starke Medikamente und daher blinzele ich oft, der Müdigkeits-Assistent erkennt dies als Dauermüdigkeit. Muss ich dann meiner Kfz-Versicherung Auskunft erteilen und ein Attest vorlegen, damit ich keine Beitragserhöhung oder gar eine Kündigung bekomme? Was geht die das an? Bis dato reicht ein Führerschein.

Eingriffe in das Verhalten des Fahrers

Die beschriebene Überwachung des Fahrers ist aber eigentlich legale Peanuts (hier können sich div. Anwälte, Richter, der ADAC und der Verkehrstag in Goslar[9] austoben) gegenüber dem, was die Industrie plant, um massiv in den Fahrvorgang einzugreifen.

Da die meisten Autos im Prinzip sehr ähnlich sind – mehrere Räder, welche normalerweise auf der Straße sind, eine Fahrgastzelle, Bedienelemente, Antrieb etc. – muss man sich eben immer mehr Features einfallen lassen, um die Produkte an den Konsumenten zu bringen und gemäß dem Grundsatz „Gier frisst Hirn“ (auch bekannt als Shareholder Value) werden hier sehr gefährliche Ideen implementiert.

Wie so oft begann diese Entwicklung ganz schleichend mit einfachen mechanischen Systemen wie Gurtstraffern und Ähnlichem. Dabei waren diese nicht ungefährlich: Ein Freund von mir hat mehr als eine Sonnenbrille dem Gurtstraffer opfern müssen. Er hat sich, halb auf dem Fahrersitz sitzend, gebückt und der (amerikanische) Gurtstraffer zog die Tür zu und stieß die Brille von seiner Nase: Brille hin, Nase kaputt.

Mit der Zeit wurden diese Features elektronisch erweitert: Gurtstraffer mit Kollisions-Sprengladungen um den Fahrer in den Sitz zurückzuholen. Oder diese Autos, die nett zum Fußgänger-Opfer sein wollen: Unter der Motorhaube lauern dann Sprengladungen, die beim Aufprall die Motorhaube heben und das Opfer über das Auto hinwegschleudern, mit ein wenig Pech dann eben vor den hinterherfahrenden Linienbus, welcher nicht ganz so nett zu Fußgängern ist.

Der Vater eines Freundes hat es auch geschafft, mit einer ruckartigen Bremsung diese Sprengung ganz ohne Gegner auszulösen. Der Schaden am Auto belief sich auf mehr als EUR 5.000. Er war ja auch Italiener: Die fahren eben so. Geschieht ihm doch recht, dass er nun in der Versicherung zurückgestuft wird, weil er einfach nicht begreifen will, wie cool dieses Feature wirklich ist.

Mit steigendem Integrationsgrad der Elektronik einhergehend und mit immer gewagteren Marketing-Prognosen über das, was Kunden wünschen (natürlich ohne es wirklich zu wissen…), wurden die Automatiken allumfassender und immer perfider, bis zu dem Punkt, wo sie auch in das Fahren aktiv eingreifen durften.

So ruckeln Spur-Assistenten am Lenkrad um den Fahrer darauf aufmerksam zu machen, dass er die Spur verlässt. Das motorisierte Proletariat darf sich dann mit Rüttelasphalt begnügen,

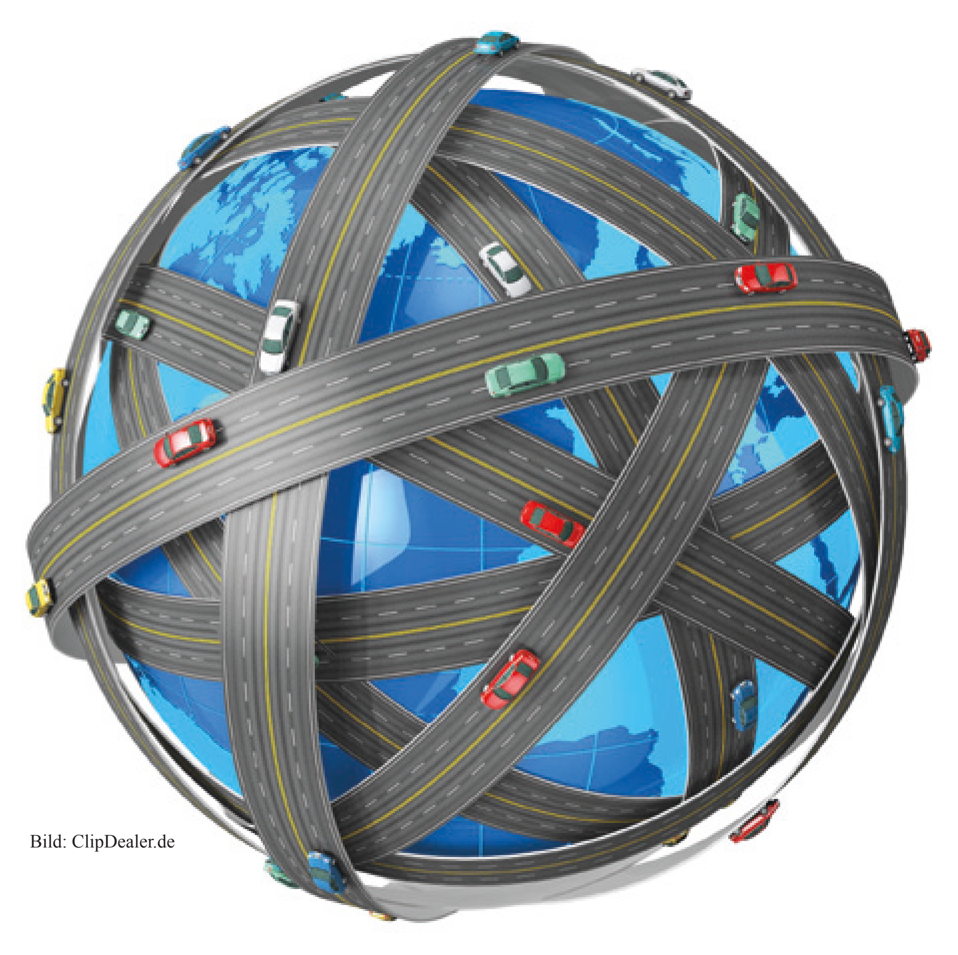


Bild: ClipDealer.de

aus dem normalerweise die Autobahn-Spuren gemalt sind. Rüttelt auch, ist effektiv, lässt sich aber leider nicht mit der kybernetischen Selbstfahrlafette als Sonderzubehör verkaufen. Falls übrigens der werte Leser der Meinung ist, es gäbe keinen Klassenkrieg auf deutschen Straßen, dann sei ihm als Lektüre die Kurzgeschichte von Harry Harrison (ca. Mitte 1960er): „Why Johnny Can't Speed"[10] empfohlen. Eine sehr präzise Analyse des Kriegs auf der Straße.

Dann gibt es bei einigen Herstellern einen Alkomaten, der es vereitelt, den Wagen zu starten, wenn im Atem des Fahrers ein entsprechender Pegel gemessen wird[11]. Ein Failure-Szenario dafür zu finden ist sehr einfach: Ich fahre mit dem werten H. Spaeing von der DVD zur redaktionellen Besprechung dieses Artikels in einen entlegenen Landgasthof. Da er fahren will, darf ich ein Weißbier oder gar zwei trinken. Auf dem Heimweg bekommt er hinter dem Steuer einen Herzinfarkt und es gelingt ihm, den Wagen rechts ran zu fahren. Ich wuchte seinen leblosen Körper auf den Beifahrersitz, kann aber aufgrund meiner vom Alkomaten gemessenen Fahruntüchtigkeit leider den Wagen nicht starten. Da wir in einer Zone ohne Handy Empfang gestrandet sind, kann ich das nett beschriftete BMW Connect Knöpfchen drücken, bis er tot ist.

Generell gilt: Es gibt jede Menge Situationen (einsetzende Wehen, Verletzungen etc.) in denen ein Fahrer mit einem messbaren Alkohol-Pegel wesentlich ungefährlicher ist als die akute Notlage. Es wäre ja gegen solche Automatiken nichts zu sagen, wenn es eine einfache, rein mechanische und von einer Verbindung zum Hersteller unabhängige Methode gäbe den Schwachsinn auszuschalten. Das darf ja dann gerne auch in der Black-Box aufgezeichnet werden, ggf. mit einem Pop-Up, dass nun die werkseitige Garantiezeit mit sofortiger Wirkung abgelaufen ist. Aber es sollte möglich sein.

Ein Freund von mir, ebenfalls Sicherheits-Berater, hat vor Kurzem ein neues Auto gekauft und der Verkäufer meinte demütig und entschuldigend, dass er sehr bedaure, aber der Wagen habe leider für die Passagiere im Fond keine elektrischen Fensterheber. Mein Freund meinte, dies sei für ihn eher ein Sicherheits-Feature, weil er die Fenster auch dann aufbekommt, wenn er mit der Karre in einen Teich fährt und der Strom ausgefallen ist. Er hat Recht.

Noch gefährlicher wird das, wenn der Wagen zum Beispiel das Verkehrsschild mit einer Geschwindigkeitsbegrenzung erkennt und nicht nur dem Fahrer zur freundlichen Beachtung seine „enhanced reality" einblendet, sondern dann bei Nichtbeachtung gleich das Tempo drosselt. Nur leider bin ich gerade dabei zu überholen und der Wagen vereitelt es, dass ich vor dem entgegenkommenden LKW noch rechtzeitig einscheren kann.

Meine blühende Fantasie lässt mich auch an von Autobahnbrücken herabhängende, gefälschte Tempo-30-Schilder denken. Einige Autos erkennen diese und bremsen. Die anderen fahren eben auf und binnen weniger Sekunden ist die Autobahn dicht.

Einige Autohersteller meinen, ihr Auto erkennte zuverlässig Fußgänger und andere Soft Targets. Auch meine auf eBay ersteigerten Schaufensterpuppen, die ich mit Schrittgeschwindigkeit in den fließenden Verkehr schiebe? Wer bremst? Wer wird von anderem Blech gebremst? Die Straße ist kein Nullsummen-Spiel: Die Summe der Schäden kann erheblich sein.

Angriffsflächen und solche, die es werden wollen

Ich verbringe viel bezahlte Zeit damit, Rechner- und Verteidigungs-Infrastrukturen im Rahmen von Pen-Tests zu überlisten und die Objekte der Begierde in einer Form zu nutzen, welche von den Entwicklern nicht antizipiert wurde. Das klappt leider überraschend gut. Bei den darauf folgenden Code Audits mit Entwicklern bin ich immer wieder erstaunt und enttäuscht, wie schlecht diese ausgebildet sind. Damit einher geht auch eine absolut uneinsichtige Ablehnung, etwas „für die Sicherheit" zu tun.

Daher bin ich zuversichtlich bis absolut sicher, dass einige der obigen Versagens-Szenarien durchaus funktionieren werden; bei einigen möchte ich, ehrlich gesagt, nicht zu nahe dabei sein.

Generell gilt: Jedes neue Software-Feature, jede Bluetooth-Verbindung,

jede GSM-Anbindung vergrößert die dem Angreifer zur Verfügung stehende Angriffsfläche.

Immens freue ich mich schon auf die „Talking Cars". Es ist ja nicht nur geplant, dass Autos immer autarker werden, sie sollen auch miteinander reden und sich gegenseitig über Gefahren wie Staus oder Aquaplaning informieren. Na, ich hoffe ja mal, die unterhalten sich ab Werk mit dem „sicheren" HTTPS-Protokoll, weil ich mir sonst mal eben die Bahn freiräume, indem ich allen Autos sage, dass auf der linken Spur ein Unfall die Spur blockiert. Während sich alle einreihen, düse ich mit 280 auf der linken Spur dann am gutgläubigen Pöbel vorbei. Astrein.

Dabei sehe ich es als meine professionelle Pflicht, darauf hinzuweisen, dass das HTTPS-Protokoll keineswegs immer sicher ist. Wie bei allen Verschlüsselungen kommt es hier stark auf die Stärke des Schlüssels, seiner Entropie-Anteile und andere Rahmenbedingungen an.

„Na sicher", höre ich schon den Autolobbyisten erbost schnaufen, „das ist doch von BMW/Mercedes/andere Nobelmarke: Die machen das sicher". Ja klar, das waren doch die, die es kürzlich verschlafen haben, überhaupt HTTPS von vornherein einzuschalten.

Wenn die Schlüssel zu einfach sind, lesen selbst schwächere Rechner die Kommunikation in Echtzeit mit. Da kann der Hersteller HTTPS im Browser anzeigen, bis der BMW Connect Knopf schwarz wird, andere lesen mit.

Diese Angreifbarkeit von Autos wirft neue Fragen auf: Wie merke ich, wenn jemand den Inhalt der Black-Box manipuliert? Wird hier das Tätigkeitsfeld der Chip-Tuner einfach pekuniär reizvoll erweitert? Wie merkt der Hersteller, dass der Wagen andere Firmware hat, als ausgeliefert, wenn zum Beispiel Signaturen gefälscht werden? Wie merkt es der Richter, vor dem ich wegen Körperverletzung mit Todesfolge im Straßenverkehr dann stehe?

Wie blockiere ich Infektionswege wie Audio-CDs[12] oder USB-Sticks in der Stereo-Anlage? Ist schon passiert, dass über diesen Weg eine Mercedes-Limousine übernommen wurde. Was ist mit TMC und dem Navi? Freunde von mir sind in der Lage, über das TMC das Navi zu steuern[13]. Entführung wird so sehr einfach. Merke: Das Navi ist ein Rechner, auf den wir grundsätzlich hören.

Selbstfahrende Autos

Wie immer ist die Branche dabei, sich selbst zu übertreffen und arbeitet mit Nachdruck an selbstfahrenden Autos. Sehr witzig. Alleine die Frage, wer denn für einen Unfall die Haftung übernimmt, wenn der Wagen, wie das Google-Auto, gar kein Lenkrad hat, welches der panische Passagier herumreißen könnte, um einen Unfall zu vermeiden, dürfte Bücher füllen und so manche Jura-Dissertation ermöglichen. (Mein Satz ist länger als Dein Satz, Hombre…)

Nun hat gerade diese intellektuelle Selbstbefriedigungsveranstaltung namens Deutscher Verkehrstag im unvermeidlichen Goslar getagt und beschlossen, dass hier natürlich alleinig der Hersteller haftet.

Irgendwie schon fast rührend, diese naive Gesetzesgläubigkeit. Erstens wird kein Hersteller Dir mehr ein Auto verkaufen, wenn Du nicht die Lizenzbedingungen anklickst (inklusive Einwilligung zur allumfassenden Datenerhebung). Kein Klick – kein Auto. Wie in der Reinigung: kein Abholzettel, kein Hemd.

Zweitens dürften TTIP und andere Abkommen solch abtrünniges Ansinnen binnen Millisekunden über ein Schiedsgericht aushebeln. Einstweilige Anordnung, Zack, Aus.

Dabei wird es sicher lustig, wenn sich das Google-Auto dann mit 40 km/h (mehr fahren die zur Zeit nicht) durch die Stadt quält, dahinter eine lange Schlange anderer fluchender Verkehrsteilnehmer. Aber halt: Fluchen darf man dann auch nicht mehr: Wird ja alles aufgezeichnet.

Sicher, sicher: Die Befürworter meinen, für Senioren wären solche autarken Autos ein riesiger Gewinn an Mobilität. Das ist sicher wahr, vereinfacht aber auch die Arbeit so manchen Sterbehilfe-Vereins…

Der investigative Journalist freut sich, wenn Autos dann gewisse, für ihn interessante Gebiete und Adressen nicht anfahren wollen und ihn gleich in die Lubjanka fahren, wo er dann leider diese fiese Steintreppe runterfällt. Oder man fährt ihn gleich von der nächsten Autobahnbrücke. War halt Software-Versagen: Schade.

Merke: Staatlich garantierte Reise- und Bewegungsfreiheit bedeutet ebenfalls: ohne staatliche Überwachung. Diese Zeiten sind wohl schon lange vorbei.

Bei einigen dieser Features und Software-Probleme der Autos ist es meiner Meinung nach keine Frage, ob jemand stirbt, nur wann und wie viele.

Die Straße ist eben kein Nullsummen-Spiel, aber die Spielregeln werden sehr bald von Robotern geschrieben. Ich bin auf den Gewinner sehr gespannt.

1 https://de.wikipedia.org/wiki/Mittlere_Datentechnik.

2 http://www.heise.de/newsticker/meldung/ConnectedDrive-Der-BMW-Hack-im-Detail-2540786.html.

3 http://www.spiegel.de/wissenschaft/weltall/yutu-china-gibt-mondsonde-jadehase-verloren-a-953116.html und natürlich auch https://de.wikipedia.org/wiki/Mondlandung.

4 http://marsrovers.nasa.gov/overview.

5 http://www.dlr.de/rosetta/.

6 https://twitter.com/nasavoyager.

7 c't, Heft 19 / 2014, Seiten 62 ff., „Schädliche Daten-Emissionen", Autorin: Christiane Schulzki-Haddouti.

8 https://de.wikipedia.org/wiki/Honi_soit_qui_mal_y_pense.

9 http://www.deutscher-verkehrsgerichtstag.de/.

10 Why Johnny Can't Speed: Heyne SF 4352 von 1984, auch als Ebook erhältlich.

11 http://www.autobild.de/artikel/toyota-testet-alkomat-an-bord-980492.html und http://www.alkomat.net/index.php.

12 http://www.itworld.com/article/2748225/security/with-hacking--music-can-take-control-of-your-car.html.

13 MC Hacking: Vortrag IT-Defense 2008, Andrea Barisani und Daniele Bianoc: Hacking Vehicle Telematics: Injecting RDS-TMC Traffic Information".

Franziska Facius

Die Verordnung der Regeln über die Einführung von bordeigenen eCall-Systemen in Fahrzeugen – ein Datenschutz-Papiertiger?

Die Telematik ist in neuen Fahrzeugen fester Bestandteil. Viele Fahrer haben sich an die Vorzüge von Außenbordkameras, Navigation und Fahrerassistenzen gewöhnt und wollen diese nicht mehr missen. Doch wir alle wissen, dass diese Anwendungen auch Gefahren in sich tragen. Durch die telematischen Einrichtungen im Auto können der Fahrer, seine Fahrweise und seine Bewegung im Straßenverkehr vollständig überwacht werden. Der Fahrer kann die Telematikanwendungen nicht selbst abschalten. Sie arbeiten unabhängig von seinem Nutzungswillen autonom.

Der eCall als Telematikanwendung im Auto soll als technische Errungenschaft zum Nutzen der Fahrer und Insassen eingesetzt werden. Dieses Ziel hat sich die Europäische Union bereits vor circa 10 Jahren gesetzt. Nach Einschätzung der EU-Kommission können so bis zu 2500 Menschenleben jährlich gerettet werden. Die Rettung kann wegen einer geschätzten Verringerung der Reaktionszeit um 50% wesentlich schneller erfolgen. Der eCall kann keine Unfälle verhindern, er kann aber die Rettung wesentlicher effektiver machen, so die EU-Kommission in ihrer zusammenfassenden Stellungnahme.[1]

Die Kommission begründet das Gesetzesvorhaben auf EU-Ebene mit der Zunahme grenzüberschreitender Straßenfahrten und der Tatsache, dass die Kontinuität eines eCall-Dienstes in ganz Europa durch einen einzelnen Mitgliedsstaat nicht gewährleistet werden könne.[2] Es bestünden zwar private Dienste in einzelnen Mitgliedsstaaten, diese seien aber nicht in ganz Europa verfügbar. Schließlich könne nur ein auf gemeinsamen Normen beruhendes Vorgehen einen eCall-Dienst in ganz Europa gewährleisten.[3]

Um das System europaweit zu etablieren, zur Herstellung einen Standards und der damit einhergehenden Harmonisierung des Marktes soll der eCall in Fahrzeugen deshalb verpflichtend sein.

Was genau ist der eCall?

Als eCall wird eine Notrufverbindung über Mobilfunknetze mittels in einem Kraftfahrzeug eingebauten Einrichtungen unter Aussendung eines Notrufs an die Notrufnummer 112 bezeichnet, so auch § 2 Nr. 1 NotrufV (Verordnung über die Notrufverbindung). Bei schweren Unfällen wird der Notruf automatisch gesendet; andernfalls kann der Fahrer manuell einen Notruf senden.

Durch den Notruf des eCall-Systems im Fahrzeug wird ein sogenannter Min-



eCall – ein im Prinzip nützliches, aber nicht ganz unproblematisches Notruf-System

Bild: ClipDealer.de

destdatensatz[4] an die Rettungsleitstelle gesendet. Der genaue Inhalt des Mindestdatensatzes wurde bereits durch das europäische Komitee für Normung festgelegt.[5]

Die Europäische Norm ist von allen EU-Staaten bereits in nationale Normungen übernommen worden.[6] Der Inhalt des Mindestdatensatzes besteht danach aus einem Kontrolldatensatz (identifiziert das System), der Fahrzeugidentifikationsnummer, einem Zeitstempel und den GPS-Koordinaten mit zusätzlicher Fahrtrichtungsanzeige. Als optionale Daten können das Fabrikat, Modell, Farbe, Anzahl der Insassen gesendet werden. Der Mindestdatensatz darf nur Daten einer maximalen Größe von 140 Bytes senden[7].

Bei der Sendung eines eCalls wird der Mindestdatensatz nach der deutschen Verordnung über Notrufverbindungen (NotrufV) dann über das Mobilfunknetz durch einen kostenlosen Notruf an die nach Landesrecht festgelegten Notrufabfragestellen weitergeleitet. Die technischen Einzelheiten der Notrufverbindung werden im TR Notruf (technische Richtlinie Notrufverbindungen)[8] auf der Grundlage des § 108 Abs. 3 TKG und unter Berücksichtigung der Verordnung über Notrufverbindungen geregelt.

Stand des Gesetzgebungsverfahrens

Bei einer verpflichtenden Einführung des eCall-Systems kann der Fahrer weder über den Einbau noch den Gebrauch des eCall-Systems bestimmen. Die gesetzlichen Regelungen müssen den Datenschutz und die Privatsphäre des Nutzers wahren und diesen Schutz dauerhaft und nachprüfbar sicherstellen. Eben wegen dieser hohen Anforderungen dauert das europäische Gesetzgebungsverfahren an. Seit Dezember 2014 liegt eine Einigung von Parlament, Kommission und Rat über den genauen Inhalt der Verordnung vor.

Der nunmehr vorliegende Entwurfstext der Verordnung hat einen langen Verhandlungsweg beschritten und begann im Jahre 2012, als das Europäische Parlament den Bericht „eCall: ein neuer Notruf 112 für die Bürger“[9] billigte und die Kommission aufforderte, einen Vorschlag zu unterbreiten. Dem folgte die Kommission sodann im Jahr 2013.[10]

Der Vorschlag der Kommission wurde durch das Europäische Parlament nicht ohne Änderungen am 26.02.2014 angenommen. In der legislativen Entschließung wurde durch das Parlament unter anderem gefordert, dass sichergestellt wird, dass der Notruf über die Nummer 112 kostenlos zur Verfügung steht und die Geräte zwecks Reparatur und Wartung jeder Werkstatt kostenlos, d.h. ohne Lizenz, zugänglich sein müssen.[11]

Die Verordnung soll vorgeben, dass der Mindestdatensatz durch das eCall-System so gespeichert wird, dass er vollständig gelöscht werden kann und vor allen Dingen keine dauerhafte elektronische Verfolgung des Fahrzeugs möglich ist oder sogar erfolgt. Hier war vor allem Streitpunkt, dass das eCall-System sozusagen nicht im Schlummermodus die ganze Zeit aufzeichnet, sondern sich erst bei einem Unfall einschaltet.[12]

In der allgemeinen Ausrichtung des Europäischen Rates vom 19.05.2015 wurden weitere Änderungen der Verordnung durch den Rat gefordert.[13]

Am 17.12.2014 kam es dann aufgrund der Verhandlungen zwischen Kommission, Europäischen Parlament und Europäischen Rat im sog. Trilog zu einer politischen Einigung. Nach dieser Einigung ist vorgesehen, dass das Parlament und der Rat in diesem Jahr die Verordnung endgültig beschließen.

Datenschutzstandard und Überwachung

Bereits beim ersten Hinweis auf die mögliche Einführung eines eCall-Systems in Fahrzeugen wurden mit Blick auf den Datenschutz Bedenken erhoben und Nachbesserungen gefordert. Nach dem jetzt vorliegenden Vorschlag sollen die Hersteller von eCall-Systemen gewährleisten, dass das System nicht dazu benutzt werden kann, das Fahrzeug zu verfolgen und eine dauerhafte Verfolgung nicht stattfindet.

Um dies zu erreichen, sollen die Daten auf dem eCall-System kontinuierlich gelöscht werden und nur die letzten drei Positionen des Fahrzeugs gespeichert werden dürfen, soweit es für die Bestimmung der Position und der Fahrtrichtung zum Zeitpunkt des Vorfalls unerlässlich ist.

Ferner sollen die Systeme sicherstellen, dass die Daten nur von bordeigenen Systemen zugänglich sind und nicht nach außen gelangen. Schlussendlich sollen die Hersteller ebenso gewährleisten, dass durch Privacy by design der Datenschutz gewährleistet ist.[14]

Zudem soll der Nutzer umfassende Informationen über die Datenübermittlung und Verarbeitung als Teil der Betriebsanleitung erhalten. Hierunter zählen nach der Verordnung in der aktuell vorgeschlagenen Fassung Informationen über die Rechtsgrundlage der Datenverarbeitung, über die Art der erhobenen und verarbeiteten Daten und über die Datenempfänger. Ebenso sollen die Nutzer die Information erhalten, dass das eCall-Gerät standardmäßig automatisch aktiviert wird und dass keine dauerhafte Verfolgung des Fahrzeugs erfolgt.[15]

Zu hinterfragen ist, ob die Information über die Funktionsweise des Systems in der Betriebsanleitung ausreichend ist. Nicht jeder Fahrer liest sich vor Antritt seiner Fahrt das Betriebshandbuch durch. Um auf das System hinzuweisen, wäre ein Hinweis im Innenraum des Fahrzeugs, ggf. durch einen Aufkleber, dass ein eCall-System eingebaut ist, als zusätzliche Information wünschenswert. Dann kann sich der Nutzer selbst entschließen, ob er nähere Informationen hierzu erlangen möchte oder nicht.

Standardschnittstelle für Zusatzdienste ist problematisch

Äußerst problematisch ist die nunmehr in der Verordnung aufgenommene Ausgestaltung der Standardschnittstelle des eCall-Systems für Zusatzdienste.

Der Entwurf sah und sieht einen obligatorischen Einbau eines bordeigenen eCall-Systems vor. Vorteil einer verbindlichen Einführung sei auch, so die Kommission in ihrem Entwurf, dass der Dienst allen Bürgern zugänglich gemacht würde und nicht auf Fabrikate einer bestimmten Preisklasse beschränkt sei. Sicher ist es lobenswert, einen einheitlichen Basisstandard für alle Fahrer zu schaffen, gleichzeitig sollen aber auch unabhängige Anbieter weiterhin zusätzliche Notfalldienste neben dem verpflichtenden eCall bereitstellen und anbieten können. Dies soll über eine Standardschnittstelle in dem System erreicht werden. Hier wird die Gleichheit wieder aufgehoben und offenbart

ein weiteres Ziel der EU: Der Markt soll wettbewerbsfähig sein und aufgewertet werden. So heißt es in dem zusammenfassenden Bericht der Kommission:

„Außerdem würden der Telematikmarkt und die Nutzung von GNSS-/Galileo-Empfängern in Europa einen Aufschwung erfahren, was zu einem indirekten Nutzen führt.“[16]

Auch in dem Verordnungsvorschlag der Kommission heißt es: „[…] Innovationen zu fördern und die Wettbewerbsfähigkeit der europäischen Informationstechnologie auf den Weltmärkten zu stärken.“[17]

Einerseits sollen die Hersteller für den Fall, dass private Dienste mit Zusatznutzen bereitgestellt werden, sicherstellen, dass ein Austausch von personenbezogenen Daten zwischen diesen nicht möglich ist. Andererseits wird jedoch gefordert, dass die bordeigenen eCall-Systeme so konzipiert sein sollen, dass sie offene Plattformen für bordeigene Anwendungen oder Dienste sind, um die Wahlfreiheit der Kunden und eine faire Wettbewerbsbedingung zu gewährleisten. Es sollen Innovationen gefördert und die Wettbewerbsfähigkeit der europäischen Informationstechnologie-Branche auf den Weltmärkten gestärkt werden. Zumindest gesteht der Verordnungsentwurf jedoch ein, dass es die hierzu nötigen technischen und rechtlichen Grundlagen noch nicht gibt, diese also erst geschaffen werden müssen.[18] Hierzu hat die EU-Kommission eine Ermächtigung erhalten, Verordnungen zu erlassen und gegebenenfalls Gesetze auf den Weg zu bringen.

Als Ergebnis bleibt festzuhalten, dass mit der verbindlichen Einführung eines eCall-Systems auch eine offene Schnittstelle für Zusatzdienste geschaffen wird. Wie dies mit den Anforderungen an die Hersteller von eCall-Systemen in Einklang gebracht werden kann, ist offen, da sich dieser Widerspruch nicht im Gefüge der bereits bestehenden europäischen und nationalen Verordnungen und Gesetze auflösen lässt.

Die Systeme können und sollen nicht ausschließlich durch die Hersteller gewartet werden. Demnach können die Hersteller nur gewährleisten, dass die Geräte bei der Auslieferung den Anforderungen der eCall-Verordnung entsprochen haben. Wer alsdann Veränderungen vornimmt und Zusatzdienste über die Schnittstelle installiert, hat auch Zugriff auf die Konfiguration der Geräte.

Die Problematik der Schnittstelle wurde bereits durch den Europäischen Datenschutzbeauftragten mehrfach in seinen Stellungnahmen aufgezeigt.

So führte der EDSB bereits frühzeitig aus: „Das vom Vorschlag vorgegebene System ist ein offenes System und unterschiedslos auch Dritten für Reparaturen und Wartung zugänglich und dient außerdem als Plattform für von Dritten angebotene Mehrwertdienste. Könnten solche Dienste die technischen Möglichkeiten der in jedem Neuwagen eingebauten Ausrüstung in vollem Umfang nutzen, würde dies erhebliche zusätzliche Risiken für die Privatsphäre bedeuten, vergleichbar mit denen durch Apps auf Smartphones.“[19]


Bild: ClipDealer.de

Frage der datenschutzrechtlichen Einwilligung bei Zusatzdiensten

Unklar sind zudem die Anforderungen an die datenschutzrechtliche Einwilligung für die Zusatzdienste. Auch hierauf hatte der EDSB bereits hingewiesen und führte in seiner Stellungnahme aus. „Der EDSB hält daher fest, dass der derzeitige Wortlaut der Verordnung zwar das Potenzial anerkennt, das sich Automobilherstellern mit dem bordeigenen eCall-System bietet, dass er aber keine Aussagen zu den Auswirkungen auf den Datenschutz enthält und damit eine ungeregelte Entwicklung dieser Systeme ermöglicht und auf diese Weise eine Regelungslücke schafft.“[20]

Wichtig ist, dass die Anbieter von Zusatzdiensten vorab die Einwilligung des jeweiligen Fahrers oder sogar der Insassen einholen müssen. Eine solche Einwilligung muss der Nutzer in vollständiger Kenntnis aller für ihn relevanten Umstände und ohne Zwang abgeben. Allgemeine Geschäftsbedingungen oder eine Einwilligungserklärung im Zusammenhang mit dem Erwerb des Fahrzeugs genügen diesen Anforderungen nicht. Nur durch eine eindeutige rechtliche Vorgabe zur Einwilligung und die Festlegung, dass deren Verweigerung für den Fahrer nicht nachteilig ist, kann vermieden werden, dass die vermeintlich zusätzlichen Dienste sich für den Benutzer nicht ins Gegenteil verkehren und letztlich beispielsweise dem Automobilhersteller, den Versicherungen oder der Pannenhilfe in die Hände spielen.

Schließlich muss auch eine verbindliche Regelung über die Geltungsdauer der Einwilligung bestehen sowie die Möglichkeit, die Einwilligung unkompliziert und ohne Nachteile zurückzunehmen.

Wer überwacht das System?

Letztlich stellt sich vor allen Dingen auch die Frage, inwieweit eine Überwachung der Anbieter von eCall-Systemen bzw. Zusatzdiensten möglich ist, so dass eine Missachtung der Vorgaben zu einer Sanktion des Herstellers führen kann.

Art. 10 der Verordnung stellt zunächst fest, dass die Mitgliedsstaaten Verstöße von Herstellern gegen die Vorschriften mit konkreten Sanktionen ahnden sollen, welche diese festzulegen haben. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Nunmehr ausdrücklich aufgeführt sind Verstöße gegen die Bestimmungen der Privatsphäre und des Datenschutzes.[21] Bevor ein Verstoß sanktioniert werden kann, muss er jedoch zunächst festgestellt werden. Die umfassende technische Überwachung des eCall-Systems durch den Nutzer selbst dürfte schlichtweg aufgrund der notwendigen Sachkunde

nicht realisierbar sein. Eine Prüfung könnte nur über ein eigenes Prüfsystem ermöglicht werden.

Wenn aber dem Nutzer eine eigene Überprüfung nicht möglich ist, muss er sich auf die Angaben des Herstellers verlassen können. Verlässt er sich nicht, muss er sich wohl fachkundige Prüfung einkaufen. Dies wäre dann ein weiterer Effekt der Verordnung für die europäische Dienstleistungsbranche.

Die Art und Weise der Sanktionierung solcher Datenschutzverstöße wäre durch Rechtsnormen der Mitgliedsstaaten zu klären. Bei einem offenen System kann eine datenschutzrechtlich relevante, nachteilige Veränderung des eCall-Systems letztlich von vielen Akteuren verursacht worden sein.

Fazit

Den Vorteilen eines europaweit einheitlichen eCall-Systems steht die Gefahr gegenüber, dass dieses System zur Überwachung missbraucht wird, indem die technisch standardisierte Plattform auch Dritten die Nutzung von Fahrerdaten ermöglicht. Die gewollte und nützliche Harmonisierung des eCall-Systems kann so gleichzeitig tiefe Gräben für den Datenschutz ausheben, da die Zusatzdienste anderen gesetzlichen Regelungen unterfallen und so keine einheitliche Datenschutzgesetzgebung für Telematikanwendungen in Kraftfahrzeugen bestünde.

Nach dem jetzigen Verordnungsentwurf dürfen 36 Monate nach Inkrafttreten der Verordnung neue Fahrzeugtypen nur dann eine Typengenehmigung erhalten, wenn sie mit einem eCall-System entsprechend der Verordnung ausgerüstet sind.

Ob das System ab 2018 verpflichtend eingeführt wird, kann erst die Zukunft zeigen. Nicht nur die Autohersteller müssen bis dahin noch viele Hausaufgaben erledigen. Auch die Mitgliedsstaaten selbst müssten nationale Regelungen erlassen, Standards abstimmen und die Notrufsysteme organisieren.

Offen ist derzeit auch die Position des Vereinigten Königreichs zu der Verordnung. Dieses erhält weiterhin den allgemeinen Vorbehalt zum gesamten Vorschlag aufrecht und würde es vorziehen, wenn der Einbau von eCall-Systemen in Neufahrzeugen ins Ermessen der Hersteller gestellt bliebe.

Nach alledem ist die eCall-Verordnung kein Papiertiger sondern eher ein Wolf im Schafspelz.

1 Arbeitsdokument der Kommissionsdienststellen, Zusammenfassung der Folgenabschätzung zur Einführung des harmonisierten EU-weiten bordeigenen Notrufs („eCall“), Begleitdokument zur Empfehlung der Kommission zur Unterstützung eines EU-weiten eCall-Dienstes in elektronischen Kommunikationsnetzen für die Übertragung bordseitig ausgelöster 112-Notrufe („eCalls“) Brüssel, den 08.09.2011 SEK(2011) 1020 endgültig; {K(2011) 6269 endgültig} {SEK(2011) 1019 endgültig}, S.1.

2 S.o. S. 2.

3 S.o. S. 3.

4 MDS: minimal-data-set.

5 EN 15722:2011.

6 Übersicht der Normungen der einzelnen Länder unter: http://standards.cen.eu/dyn/www/f?p=204:35:0::::FSP_SURR_WI:32117&cs=1875E54A8E5433674E503B673CC406444.

7 EN 15722:2011.

8 Die TR Notruf (1. Auflage Stand 2011) wird durch die Bundesnetzagentur verwaltet. Abrufbar unter: http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Notruf/TechnischeRichtlinie/technischerichtlinie.html.

9 2012/2056(INI).

10 Vorschlag COM (2013) vom 13.06.2013 für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG; Vorschlag COM (2013) für einen Beschluss des Europäischen Parlaments und des Rates über die Einführung des interoperablen EU-weiten eCall-Dienstes.

11 Legislative Entschließung des Europäischen Parlaments vom 26. Februar 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung von Richtlinie 2007/46/EG (COM(2013)0316 – C7-0174/2013 – 2013/0165(COD)) (Ordentliches Gesetzgebungsverfahren: erste Lesung).

12 S.o.

13 9605/14 ENT 119 MI 411 CODEC 1233 11124/13 ENT 194 MI 558 CODEC 1506, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG, – Allgemeine Ausrichtung.

14 9605/14 ENT 119 MI 411 CODEC 1233 11124/13 ENT 194 MI 558 CODEC 1506, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG, – Allgemeine Ausrichtung.

15 ST 16345 2014 INIT; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG – Politische Einigung.

16 SEK(2011) 1019 endgültig}, S.5.

17 Vorschlag COM (2013) vom 13.06.2013 für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG; Vorschlag COM (2013) für einen Beschluss des Europäischen Parlaments und des Rates über die Einführung des interoperablen EU-weiten eCall-Dienstes.

18 ST 16345 2014 INIT; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG – Politische Einigung.

19 Stellungnahme des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typengenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG, S. 4.

20 Kommentare des EDSB zur Empfehlung der Kommission und der dazugehörenden Folgenabschätzung der Umsetzung des harmonisierten EU-weiten bordeigenen Notrufsystems („eCall“), 2012.

21 ST 16345 2014 INIT; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung der Richtlinie 2007/46/EG – Politische Einigung

Christian Siedenbiedel

Belohnung für vorbildliche Autofahrer

Abdruck aus der Sonntagszeitung, 23.11.2014, GELD & MEHR (Geld und Mehr), Seite 31 – Ausgabe D1, D1N, D1S, D2, R

„Wer vorsichtig fährt, kann künftig bei der Kfz-Versicherung sparen. Ein digitaler Beifahrer überwacht den Fahrstil. Lohnt sich das?“

Warum müssen rasante und leichtsinnige Autofahrer bei der Kfz-Versicherung eigentlich genauso viel zahlen wie super vorsichtige? Obwohl sie, statistisch gesehen, viel weniger Schaden verursachen? Dieses Missverhältnis wollen die ersten Versicherungen gerade ändern. Sie installieren deshalb technische Vorrichtungen in Autos, mit denen man den Fahrstil des Autofahrers kontrollieren kann. Wer vorsichtig fährt, bekommt später einen Teil seiner Versicherungsprämie zurückerstattet.

Das ist eine Revolution in der Kfz-Versicherung: Angefangen hat damit zumindest in Deutschland vor knapp einem Jahr die Sparkassen-Direktversicherung in Düsseldorf. Jetzt kommt mit der Signal Iduna eine zweite Assekuranz hinzu, die einen solchen Tarif „Pay as you drive“ („Zahle, wie du fährst“) für erste Kundengruppen anbietet. Experimente damit gibt es außerdem beispielsweise bei den Versicherungen AXA und Itzehoer. Auch die Allianz hat ähnliche Tarife schon in anderen Ländern mit einigem Erfolg ausprobiert – etwa in Italien.

Die Experimente scheinen ganz erfreulich zu verlaufen: Die Sparkassen-Direktversicherung jedenfalls hat mittlerweile 1000 Kunden, die einen solchen Versicherungsvertrag abgeschlossen haben, und führt außerdem schon eine Warteliste mit weiteren Interessenten.

Es gibt dabei unterschiedliche Modelle, wie das Ganze technisch umgesetzt wird. Bei der Sparkassen-Direktversicherung funktioniert es so: Ins Auto wird ein Kästchen eingebaut, nicht größer als ein Smartphone. Es nennt sich „Blackbox“ oder „Telematik-Box“. Es hat unterschiedliche Funktionen, unter anderem sendet es bei Unfällen automatisch einen Notruf. Am interessantesten aber ist seine Fähigkeit, Daten über den Fahrstil des Autofahrers für die Versicherung einzusammeln. Wie stark beschleunigt jemand? Wie oft legt er eine Vollbremsung hin? Fährt er zu schnell?

Alle 20 Sekunden sendet die Box dann Daten über Lage, Geschwindigkeit und Beschleunigung des Autos an ein Rechenzentrum der Telefongesellschaft Telefónica in London. Diese weiß nicht, um wen es sich bei dem Autofahrer handelt, sondern kennt nur eine sogenannte Kunden-Identifikationsnummer und speichert die Angaben ähnlich wie sonst Handydaten.

Einmal im Monat meldet die Telefongesellschaft der Versicherung einen sogenannten „Score“-Wert: die Bewertung des Fahrstils. Macht man alles perfekt, bekommt man 100 Punkte. Abzüge gibt es nicht nur für verbotene Geschwindigkeitsübertretungen, sondern auch für Verhaltensweisen, von denen die Versicherungsmathematiker sagen, dass sie statistisch für ein höheres Unfallrisiko stehen. Dazu gehört starkes Beschleunigen oder extremes Bremsen. Auch wer oft nachts fährt, gehört in eine Risikogruppe und bekommt Abzüge. Genauso wie Menschen, die vor allem in der Stadt unterwegs sind, wo es häufiger kracht als auf dem Land.

Die Versicherung ordnet diese Score-Werte dann anhand der Kundennummer ihren Versicherten zu. Wer in einem Monat mehr als 80 Punkte schafft, bekommt fünf Prozent Rabatt bei der Versicherungsprämie. Außerdem wird einmal im Monat der vorbildlichste teilnehmende Autofahrer ermittelt („Fahrer des Monats“), der dann ein Quartal lang sogar kostenlos versichert wird. Keine Frage: Es geht dabei auch um die Erziehung der Fahrer.

So richtig zu lohnen scheint sich eine solche Art von Versicherung allerdings nur für die Halter großer Autos. Je nach Vertriebsweg zahlt man für die Technik eine Miete von bis zu 71,40 Euro im Jahr. Der Rabatt bringt deshalb nach den bisherigen Erfahrungen vor allem etwas bei Autos vom Geländewagen BMW X6 an aufwärts. Es sei denn, der Halter eines kleineren Autos schätzt vor allem den Nutzen von zusätzlichen technischen Funktionen der Blackbox – wie der Möglichkeit, das Auto nach einem Diebstahl zu orten oder dem automatischen Notruf an den Rettungswagen nach einem Unfall.

„Das System ist stabil und das Feedback unserer Kunden hervorragend“, sagt jedenfalls Jürgen Cramer, Vorstandsmitglied der Sparkassen-Direktversicherung.

Offenbar ist die Schwelle, ab der man Geld von der Versicherung zurückbekommt, moderat gewählt worden. „Etwa drei Viertel der Teilnehmer kommen auf mehr als 80 von 100 Scoring-Punkten – und bekommen damit eine Ermäßigung im Tarif“, sagt Cramer.

Ob die Autofahrer, die sich das kleine Kästchen ins Auto einbauen lassen, genau deshalb besonders vorsichtig fahren, oder ob sich nur besonders vorsichtige Fahrer so ein Kästchen überhaupt einbauen lassen, ist dabei nicht leicht zu klären.

Sicher aber ist: Die Versicherung kann jetzt das Fahrverhalten ihrer Kunden besser abschätzen. „Punktabzug gab es am häufigsten wegen eines zu rasanten Fahrstils“, sagt Vorstand Cramer. „Gefolgt von Geschwindigkeitsübertretungen.“ Beides traf wohl ähnliche Autofahrer-Gruppen.

Für die Versicherung ist das Ganze nach wie vor ein Pilotprojekt. Ob daraus

ein Standard-Angebot wird, habe man noch nicht entschieden, sagt Cramer.

Zu den größten Sorgen der Kunden bei solchen Angeboten von Versicherungen gehört zweifellos der Datenschutz. Die Vorstellung, dass im Auto gleichsam immer ein digitaler Beifahrer dabei ist, der jede kleine Verkehrssünde sieht und ahnden kann, wird vielen freiheitsliebenden Menschen zumindest ein gewisses Unwohlsein bereiten. Soll die Versicherung wirklich jeden meiner Wege kennen?

Bei der Sparkassen-Direktversicherung verweist man darauf, dass man genau aus solchen Überlegungen heraus die erhobenen Daten sehr sorgfältig trennt. Die beiden getrennten Datenkreise bei der Versicherung und der Telefongesellschaft, die nur über die Kundennummer verbunden sind, sollen dafür sorgen, dass keines der beiden Unternehmen kontrollieren kann, wo ein Autofahrer gerade steckt. „Wir haben vom Landesbeauftragen für Datenschutz bescheinigt bekommen, dass unser System die Anforderungen an den Datenschutz erfüllt“, sagt Cramer.

Trotzdem: Ein gewisses Unbehagen bleibt. Grund genug für die Konkurrenz-Versicherung Signal Iduna, die jetzt etwas Ähnliches anbietet, genau an diesem Punkt anzusetzen. „Bei uns werden keine Daten erhoben, welcher Autofahrer gerade wo langfährt“, sagt John-Sebastian Komander von der Iduna-Tochtergesellschaft Sijox. „Das ist uns sehr wichtig.“

Dieses zweite Modell des fahrstilabhängigen Versicherungstarifs funktioniert deshalb anders – und richtet sich auch an eine andere Zielgruppe. Sijox ist auf junge Leute spezialisiert. Und das neue Angebot soll auch vor allem Fahranfänger, die gerade ihren Führerschein gemacht und ihr erstes Auto bekommen haben, zu gutem Fahrverhalten erziehen.

Mitmachen kann man überhaupt nur, wenn man zwischen 17 („Führerschein mit Siebzehn“) und 30 Jahre alt ist. Und vertrieben werden diese Versicherungspolicen ausschließlich von jungen Versicherungsvertretern.

Passend zur Zielgruppe funktioniert die Kontrolle des Fahrstils dabei über eine App auf dem Smartphone. Die jungen Autofahrer oder ihre Eltern können ein „Dongle“ genanntes kleines Gerät bestellen. Das steckt man (nach einer Anleitung aus dem Internet) im Auto auf eine Schnittstelle zur Bordelektronik des Autos.

Über Bluetooth überträgt dieses Gerät dann bestimmte Daten über den Fahrstil wie Bremsungen, Beschleunigen und das Tempo in der Kurve an eine App namens „AppDrive“. Sie stammt vom Navi-Anbieter Tomtom. Dieses Unternehmen speichert die Daten dann auch auf einem (in Deutschland stehenden) Server.

Ähnlich wie bei der Sparkassen-Direktversicherung bekommt die Versicherung regelmäßig nur zusammengefasste Daten – einen Score zwischen 0 und 100 Punkten. Von 50 Punkten an gibt es dann für den jungen Versicherten eine Ermäßigung beim Versicherungstarif. Von 90 Punkten an beträgt sie immerhin 25 Prozent der Versicherungsbeiträge. Eine Miete zahlt man für die Technik nicht – und auch die App kann man sich gratis herunterladen.

„Wir wollen dieses Angebot zunächst einmal mit 500 unserer Kunden testen“, sagt Sijox-Sprecher Komander. Aus seiner Sicht ist das Angebot auch deshalb für junge Fahrer besonders interessant, weil diese ansonsten überdurchschnittlich hohe Beiträge in die Kraftfahrzeugversicherung einzahlen müssen.

Erst mit mehreren Jahren Fahrerfahrung ohne größere Unfälle steigt man schließlich in den klassischen Schadenfreiheitsklassen langsam auf – und dann wird die Versicherung automatisch billiger. Wenn jetzt junge Fahrer aber vorsichtig fahren und das durch „AppDrive“ belegen können, sollen sie schon früher an günstigere Tarife kommen.

Die Signal Iduna rechnet das an einem Beispiel vor: Ein Fahranfänger mit einem neuen Golf zahle schnell 1000 bis 2000 Euro Versicherung im Jahr. Darin spiegele sich vor allem die hohe Wahrscheinlichkeit von Unfällen und kleineren Pannen in der Zeit des ersten Ausprobierens nach dem Führerschein. Wenn jemand sich auf die Kontrolle durch die App einlasse, könne er leicht 250 oder auch 300 Euro im Jahr sparen. „Das lohnt sich ganz ordentlich.“

Dabei wird nicht einfach das, was die jungen Leute nachher sparen können, vorher auf den Tarif aufgeschlagen. Das zumindest versichert die Versicherung: Die Tarife, die man dabei ansetze, lägen „im Mittelfeld der branchenüblichen“.

Einen Preis allerdings hat die Lösung der Signal Iduna im Vergleich zur Lösung der Sparkassen-Direktversicherung: Weil keine Positionsdaten des Autos per GPS verarbeitet werden, weiß das System nicht, wer wo gerade langfährt. Das hat den Vorteil, dass der Autofahrer sich weniger kontrolliert fühlt – es hat aber auch klare Nachteile. So kann das System nicht wissen, wer Tempolimits übertritt. Es weiß schließlich zwar, wie schnell der Autofahrer fährt, aber nicht, wie viel dort gerade erlaubt ist. Es muss sich deshalb auf Kriterien wie Vollbremsungen, Kavalierstarts und hohe Kurvengeschwindigkeit beschränken. Und: Es kann im äußersten Notfall, nach einem schweren Unfall, nicht den Rettungswagen rufen: Weil es ja gar nicht weiß, wohin.


Bild: ClipDealer.de

Kann das Sytem zum sicheren Fahren beitragen?

Ob sich eines der beiden Systeme durchsetzt, und wenn ja welches, ist noch vollkommen offen. „Eine spannende Entwicklung“ nennt das auf jeden Fall der amerikanische Ökonom George Akerlof. In anderen Teilen der Welt, etwa in Amerika, gibt es bereits viel mehr Angebote der Versicherungen dieser Art. In der Branche werden zwei Gründe genannt, warum viele Versicherungen in Deutschland noch zögern. Ein Grund ist, dass die Kfz-Versicherungsprämien in Deutschland niedriger sind als in vielen anderen Ländern. Man kann durch vorsichtiges Verhalten weniger sparen. Zudem gibt es bereits viel mehr Differenzierungen der Tarife als in anderen Staaten – eine weitere Differenzierung lohnt sich weniger.

Maria Koch – Lea Rothmann

Privatheit verhandeln
Die Smartifizierung der beruflichen Mobilität

Unsere Mobilität soll smarter werden. Das heißt, sie soll durch vernetzte Telekommunikationsmedien beschleunigt, vereinfacht, ökologisch und ökonomisch nachhaltig organisiert und sicherer gemacht werden (vgl. Schmidt/Takeda/Abut/Hansen 2014; Schuh/Stich 2013; Lemke/Paar/Wolf 2006). Das gilt umso mehr für Unternehmen. Smarte Systeme werden als ein unterstützendes Medium für ein effizientes Mobilitätsmanagement gewertet. Besonders Elektromobilität, die sich „rechnen" soll, basiert auf Informations- und Kommunikationstechnologie (IKT)-gestützten Überwachungs- und Kontrollsystemen. Zur effizienten Auslastung der Elektrofahrzeuge gilt es, diese in ein System einzubinden, das es erlaubt, den Zustand eines jeden zu überwachen und passgenaue Routen für optimale Anwendungszwecke zu finden (Vidačkovič u. Weiner 2013). Dadurch wird ein umfassendes Management der gewonnenen Daten notwendig (vgl. Raabe et al. 2011). Dieser Umstand wirft besonders im betrieblichen Kontext hochbrisante Fragen zum Datenschutz innerhalb der Unternehmen im Allgemeinen und der Wahrung der Privatsphäre der Mitarbeiter/-innen im Speziellen auf (vgl. Böker u. Demuth 2013).

Der Fokus des Beitrages liegt auf den subjektiven Herausforderungen und Fragen, denen sich insbesondere Nutzer/-innen in smarten Fuhrparksystemen in Bezug auf den Schutz ihrer Privatsphäre stellen. Datengrundlage unseres Aufsatzes ist das von der Bundesregierung im Rahmen des Schaufenster Elektromobilität Berlin ressortübergreifend finanzierten Verbundprojekts „eFahrung. Unternehmensübergreifende Nutzung von E-Fahrzeugen in Unternehmensflotten". Zur Analyse der Anforderungen an die Privatsphäre in intelligenten Firmenflotten wurden deutschlandweit 90 qualitative, leitfragengestützte Experteninterviews im Zeitraum von November 2013 bis Mai 2014 geführt. Die leitfragengestützten Interviews erlauben Einblicke in die Arbeits- und Mobilitätswelt, wie sie von den Interviewpartner/-innen thematisiert wird. Der Artikel basiert auf der Studie zu den Anforderungen an Privatsphäre und Datenschutz aus Nutzer/-innen-Perspektive, die im Rahmen der sozialwissenschaftlichen Begleitforschung zum Projekt von der Technischen Universität Berlin unter der Leitung von Prof. Dr. Martina Löw von 2013 bis 2014 durchgeführt wurde. Es werden im Folgenden die Risiken und Reibungspunkte, die sich in Bezug auf die Bewertung der Privatsphäre ergeben, skizziert und Möglichkeiten für einen sozial nachhaltigen Einsatz von IKT in der Arbeitsumwelt vorgestellt.

Worum geht es?

Die zunehmende Vernetzung der Fahrzeugverwaltungssysteme und der Einsatz intelligenter Fahrzeugtechnik gelten Mobilitätsexpert/-innen als entscheidende Mittel zur Effizienzsteigerung der Mobilität. Sie sind wichtiger Bestandteil der Sicherheitssysteme, wenn es um die rechtliche Absicherung der Beschäftigten oder um die Minimierung physischer Risiken in ihrer beruflichen Mobilität geht (vgl. Scheuer 2013). Die modernen vernetzten Kommunikationssysteme im Fahrzeug sollen sowohl dazu beitragen das jeweilige Mobilitätsmedium bedarfsgerecht einzusetzen als auch die Gewohnheiten der Fahrer/-innen zu verändern und einen positiven Einfluss auf ihr Fahrverhalten zu nehmen. Das heißt, Informationen über das Fahrzeug und das Fahrverhalten in Echtzeit zu gewinnen, auszuwerten und beispielsweise dem/der Fahrer/-in noch während der Fahrt zurückzuspielen. Die Hoffnungen aufseiten der Mobilitätsmanager/-innen und vieler Mobilitätsexpert/-innen in Bezug auf smarte Datenverwaltungs-Systeme beziehen sich auf einen effizienteren Einsatz und Auslastung der Fahrzeuge, eine leichtere Kombination mit anderen Mobilitätsoptionen und die Optimierung des Fahrverhaltens der Beschäftigten. Damit ließe sich Gutes für die Umwelt tun, die Sicherheit im Straßenverkehr erhöhen, Kraftstoff sparen und gleichzeitig die Wirtschaftlichkeit des Fahrzeugs steigern.

Risiken

Dem Nutzen stehen jedoch Risiken, besonders auf der Seite der Wahrung der Privatsphäre und Persönlichkeitsrechte der Beschäftigten gegenüber. Die Sorge, die Betroffene mit der Vernetzung von Datenquellen wie Fahrzeugen, Smartphones oder anderen smarten Endgeräten verbinden, ist einerseits der Kontrollverlust der Betroffenen über ihre persönlichen Daten und damit die Gefahr der Verletzung der Integrität und Autonomie der Person. Ein besonderes Problem stellt hier der niedrige Grad an Informiertheit der befragten Akteure im Unternehmen dar. Oft wissen weder die Nutzer/-innen noch die Fuhrparkleitung, mit welchen Telematik- und IKT-Systemen die E-Dienstfahrzeuge ausgestattet sind und welche Daten von wem zu welchem Zweck erhoben werden. Das Problem für die Beschäftigten in den befragten Unternehmen ist jedoch nicht nur die mögliche oder tatsächliche Erhebung von Daten, die Rückschlüsse auf ihre Person zulässt, sondern auch der häufig mit der Einführung smarter Systeme verbundene erhöhte Leistungsdruck. Das heißt, Beschäftigte und deren Vertretung thematisieren in diesem Zusammenhang auch die steigenden Anforderungen an das Know-how, die

Produktivität, Effizienz, Flexibilität der Beschäftigten, die als Belastung und teilweise auch als Überforderung empfunden werden (vgl. DAK 2014). Die Interviewten befürchten, dass die Smartifizierung der Arbeitswelt – durch intelligente, vernetze IKT-Systeme, durch neue Mobilitäts- und Arbeitskonzepte – zu einer Entgrenzung von Freizeit und Arbeitszeit und damit auch von Privatsphäre und Öffentlichkeit führt.

Die Problematik der Entgrenzung von Privatsphäre und Öffentlichkeit zeigt sich besonders deutlich am Automobil, das als Instrument zur Herstellung von Privatsphäre gewertet wird. „Ich mache da drin, was ich will", bringt es eine Nutzerin auf den Punkt. Das macht den Personenkraftwagen für die Fahrer/-innen zu einer „Burg", „Hülle" oder „Kapsel", in der man sich geschützt und anonym durch den Verkehr bewegt. Nutzer/-innen aus unterschiedlichen Branchen, Städten, Regionen, unterschiedlichen Alters und Geschlechts schildern gleichermaßen, dass sie auch das Dienstfahrzeug als Teil ihres privaten Bereichs erleben, selbst wenn es sich um Pool- oder Nutzfahrzeuge handelt. Für einen Großteil der Befragten nimmt das Gefühl des geschützten Für-sich-Seins durch die zunehmende Kontrolle über das Fahrzeug von außen und der zunehmenden Sichtbarkeit von Handlungen in dem Fahrzeug ab. Dies ist besonders dann der Fall, wenn der Einsatz smarter Fuhrparkverwaltungssysteme vom Flottenmanagement zum Zweck der Optimierung des Fahrverhaltens der Beschäftigten eingeführt wird.

Möglichkeiten

Bei der Smartifizierung der beruflichen Mobilität handelt es sich nicht nur um eine materiell-technische, sondern auch um eine sozial-praktische und subjektiv-„gefühlte" Innovation. Der innovative Charakter der Veränderung birgt für die beteiligten Akteure ein großes Potenzial der Verunsicherung in sich. Eine Verunsicherung, die sich aus der Komplexität der smartifizierten Arbeits- und Lebenswelt ergibt, die ein Abwägen der Konsequenzen der eigenen Handlungen erschwert. Es fehlen auf allen Ebenen – Fuhrparkmanagements, Personalvertretung, Nutzer/-innen – passende Strategien im Umgang mit der Erhebung, Übertragung, Verknüpfung, Auswertung und Verwendung dieser Daten.

Um smarte Mobilitätskonzepte erfolgreich einzuführen, muss deshalb ein umfassendes Change-Management entwickelt werden, das nicht nur auf bestehende Probleme und Konflikte reagiert, sondern diese im Vorfeld verhindert. Change-Management bedeutet in diesem Fall, dass rechtliche, technische und soziale Standards, die den Wandel für alle Akteure nachvollziehbar machen und über die smarten Systeme informieren, in den Unternehmen etabliert werden müssen. Dadurch kann ein ausreichendes Maß an Transparenz für alle hergestellt werden, das ein vernünftiges Handeln in komplexen Systemen ermöglicht. Für die Smartifizierung der beruflichen Mobilität lassen sich aus den Ergebnissen des Forschungsprojektes folgende Empfehlungen ableiten:

Beschäftigte und deren Vertretungen informieren und die Verwendungszwecke smarter Medien offenlegen. Verwendungsmöglichkeiten, die nicht zur Anwendung kommen, ebenfalls kommunizieren, um eine Kultur des Vertrauens zu schaffen. Dazu bedarf es auch einer Selbstverpflichtung zum transparenten Umgang mit IKT-Systemen auf der Seite des Managements. Dabei gilt: Auch das Fuhrparkmanagement muss geschult werden, damit nicht unbeabsichtigt das Sammeln von Daten Beschäftigter durch Dritte ermöglicht wird.

Den Nutzer/-innen selbst die Mitbestimmung bei der Wahl des Mobilitätsmediums und dem Grad der Ausstattung mit IKT-Systemen zu ermöglichen, erhöht die Akzeptanz.

Privatheit ist eine kulturell und lokal variable Praxis zur Herstellung von Privatsphäre. Grenzverletzungen, Grenzüberschreitungen, Grenzakzeptanz müssen vor Ort ausgehandelt werden und individuelle Lösungen gefunden werden.

Privatsphäre, verstanden als geschützter Interaktionsraum, der durch die Privatheit (Praxis) hergestellt wird, ist eine kulturelle Errungenschaft. Wo Rückzugsräume geschaffen werden, wie kontrolliert wird, welche Aspekte der Persönlichkeit in der Handlungssituation öffentlich werden, kann variieren. Wichtig ist jedoch, dass die Schaffung von Privatsphäre auch in smarten Systemen möglich bleibt. Das heißt, dass technische, rechtliche und soziale Standards definiert und eingehalten werden.

Der Einsatz smarter Fuhrparkverwaltungssysteme geht oft mit einem Wunsch des Flottenmanagements nach einer Optimierung des Fahrverhaltens der Beschäftigten Hand in Hand. Bei der Aufforderung an die Nutzer/-innen ihr Mobilitätsverhalten zu ändern, ist immer auch mit emotionalen Reaktionen zu rechnen. Hierfür bedarf eines sensiblen, wertschätzenden Umgangs.

Konflikte können aufgrund der fehlenden individuellen Kontrolle durch die Beschäftigten sowie der kollektiven Kontrolle durch das Unternehmen beziehungsweise das Fuhrparkmanagement entstehen. Häufig verfügt Letzteres nämlich selbst nicht über das notwendige Wissen oder ausreichende Kompetenz, um auf die Verwendung der durch IKT-Systeme generierten Daten Einfluss zu nehmen. Hinzu kommt die Überforderungsproblematik: Im Umgang mit den IKT-Systemen benötigen die Beschäftigten neue Fähigkeiten zur Bedienung komplexer technischer Geräte, zum Agieren in unüberschaubaren Situationen, zum Umgang mit der Entgrenzung von Öffentlichem und Privatem. In smartifizierten Arbeits- und Mobilitätsumwelten bedarf es nicht nur der Erweiterung technischer Standards und formaler Regelungen. Es muss über die erhobenen Daten, ihre Verwendung und ihren Zweck informiert werden. Den Beschäftigten muss die Mitsprache und Mitbestimmung bei der Verwendung von IKT-Medien eröffnet werden. Den Bedürfnissen und Ängsten der Nutzer/-innen in Bezug auf die Sicherheit ihrer Daten und den Schutz ihrer Privatsphäre offen zu begegnen, ermöglicht es, Lösungen innerhalb des Unternehmens zu finden, die für alle Beteiligten zufriedenstellend sind. Es bedarf aber auch eines gesamtgesellschaftlichen Diskurses darüber, mit welchen gesellschaftlichen Werten das Konzept „Privatsphäre" verbunden wird und werden sollte. Bleibt die Privatsphäre ein für unsere Gesellschaft wichtiger Schutzbereich der Person und der mit ihr verbundenen Werte und Rechte, wie Würde, Ehre, freie Entfaltung und Unverletzlichkeit, werden wir andere Strategien im Umgang mit

den technischen Innovationen entwickeln müssen, die gerade im Bereich der Verbreitung der Telekommunikationsmedien im Alltag von unseren Befragten als Bedrohung ihrer Privatsphäre erfahren werden. Auch wenn Beschäftigte immer Teil einer Öffentlichkeit sind, bleibt ihnen das grundsätzliche Recht, ihre Persönlichkeit und die damit verbundenen Werte zu schützen. Bisher ist der Grad der Informiertheit aller an der Herstellung beruflicher Mobilität beteiligten Akteure gering hinsichtlich Risiken und Gefahren der Datengenerierung, -speicherung, -übertragung und -auswertung. Dadurch ist der Umgang mit den Systemen tendenziell krisenanfällig. Aus unserer Analyse lässt sich daher der Schluss ziehen, dass die Smartifizierung der Lebenswelt nur dann die Mobilität und Arbeit auch für Beschäftigte angenehmer und sicherer macht, wenn die smarten Interaktionsräume für diese überschaubar genug sind, um die Konsequenzen von Handlungen in gewohntem Maße einschätzen zu können.

Literaturverzeichnis

Böker, Karl-Hermann, Demuth, Ute (2013): IKT-Rahmenvereinbarung. Frankfurt am Main: Bund-Verlag.

IGES Institut GmbH (2014): DAK-Gesundheitsreport 2014.

Lemke, Kerstin/Paar, Christof/Wolf, Marko (Hg.) (2006): Embedded Security in Cars. Securing Current and Future Automotive IT Applications. Berlin/Heidelberg/New York: Springer.

Raabe, Oliver/Lorenz, Mieke/Pallas, Frank/Weis, Eva (2011): Datenschutz im Smart Grid und in der Elektromobilität. Technical Report.

Scheuer, Florian (2013): Schutz der Privatsphäre in Ad-hoc-Fahrzeugnetzen. Dissertation, Hamburg.

Schmidt, Gerhard/Takeda, Kazuya/Abut, Huseyin et al. (Hg.) (2014): Smart mobile in-vehicle systems. Next generation advancements. New York: Springer.

Schuh, Günther/Stich, Volker (2013): Smart Wheels. Mobil im Internet der Energie. FIR e. V.: Aachen.

Vidačkovič, Kešimir, Weiner, Nico (2013): Anwenderstudie: Elektrofahrzeuge im Geschäftsumfeld. Potentiale der gemeinsamen Nutzung. Stuttgart: Fraunhofer Verlag.

BfDI Pressemitteilung:

Andrea Voßhoff stellt Datenschutzinformationen in neuem Format vor

Das Informationsangebot der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurde um eine Publikationsreihe erweitert: Insbesondere für die Angeordneten des Deutschen Bundestages, aber nicht nur für sie, wurde „Datenschutz kompakt“ konzipiert. Aktuelle Themen des Datenschutzes werden hier zukünftig übersichtlich und pointiert aufbereitet. Die erste Ausgabe präsentiert den aktuellen Meinungsstand der Datenschutzbeauftragten von Bund und Ländern zum Datenschutz im Auto und greift damit ein Thema auf, das nahezu jeden betrifft. Andrea Voßhoff erläutert: „Während meiner langjährigen parlamentarischen Arbeit habe ich es immer zu schätzen gewusst, zu komplexen Themen kurze und schnelle Informationen zu bekommen. Zum einen für die parlamentarische Arbeit und zum anderen als Argumentationshilfe für die Wahlkreisarbeit oder Bürgergespräche.“ Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bietet Informationsmaterial zu verschiedenen Komplexen: Ausführliche Informationen zu den rechtlichen Grundlagen des Datenschutzes und der Informationsfreiheit als Broschüren, kurze, für jedermann verständliche Informationen zu einer Vielzahl von Themen als Faltblätter.



Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

BfDI

Datenschutz kompakt

2. Februar 2015

diesmal: *Datenschutz im Auto*

Mehrwert durch technische Innovationen in der Automobilentwicklung

Derzeit ist eine fortschreitende informationstechnische Ausstattung und Vernetzung von Kraftfahrzeugen zu beobachten, die als Weiterentwicklung des Mobile Computing verstanden werden kann. Die damit verbundenen Innovationen in der Fahrzeugtechnik sind grundsätzlich geeignet, positiv zu wirken, etwa durch ein effizientes und damit umweltverträgliches Mobilitätsmanagement oder durch ein Mehr an Sicherheit aufgrund des verstärkten Einsatzes von Assistenzsystemen. Letztlich bedeutet der technische Fortschritt in einer auf Mobilität angewiesenen Gesellschaft auch einen Komfortgewinn für den Fahrer.

Datenschutzrechtliche Gefährdungslage

Für diesen Mehrwert ist es aber erforderlich, viele Daten aus den Fahrzeugen zu nutzen. Die zunehmende Datenverarbeitung in modernen Kraftfahrzeugen und ihre Kommunikation untereinander, mit ihrer Umgebung und mit dem Internet bergen allerdings datenschutzrechtliche Risiken. Begehrlichkeiten werden geschaffen, die bei der Kfz-Nutzung anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese technischen Informationen stellen – verknüpft etwa mit der Fahrzeugidentifikationsnummer – personenbezogene Daten dar, die Auskunft über Fahrverhalten und Aufenthaltsorte geben und zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden können. Der rechtliche und tatsächliche Schutz dieser personenbezogenen Daten wird dadurch schwieriger, dass aufgrund der Vernetzung moderner Automobile mit dem Internet solche Daten in Echtzeit aus dem Fahrzeug heraus an beliebige Dritte übermittelt werden können. Dies wiederum macht es aus meiner Sicht zwingend notwendig, bei der Entwicklung sowohl von Standards zur Kommunikation von Fahrzeugen untereinander (Car-to-Car-Kommunikation) und mit ihrer Umgebung (Car-to- Infrastructure-Kommunikation) als auch von automatisierten Fahrfunktionen Aspekte des Datenschutzes und der Datensicherheit frühzeitig zu bedenken.

Forderungen der Datenschutzbeauftragten von Bund und Länder

Die datenschutzrechtliche Beratung und Kontrolle der Automobilhersteller, die letztlich für die Konzeption der in den Kraftfahrzeugen verbauten datenverarbeitenden Systeme verantwortlich sind, liegt – je nach Unternehmenssitz – in der Zuständigkeit meiner Kolleginnen und Kollegen in den Datenschutzaufsichtsbehörden der Länder. Als Vorsitzende des Arbeitskreises Verkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder bin ich intensiv mit der Koordination der Aufsichtsbehörden zu diesem wichtigen Thema befasst.

Als starkes Signal sowohl an die Öffentlichkeit als auch an die Automobilindustrie verabschiedete die Datenschutzkonferenz Anfang Oktober 2014 eine Entschließung, die im Wesentlichen folgende datenschutzrechtliche Forderungen beinhaltet:

Seite 1

Klaus-Jürgen Roth

Die CDU/CSU und der Datenschutz

Die Christlich-Demokratische Union, kurz CDU, wie auch ihre „soziale" bayerische Schwesterpartei CSU haben den Datenschutz entdeckt. Nicht, dass diese Parteien nun den digitalen Grundrechtsschutz besonders hoch halten würden. Auch nicht, dass das Thema jetzt in der Partei-Programmatik einen besonders gewichtigen Platz einnehmen würde. Man kann nicht sagen, dass besonders viele PolitikerInnen dieser Parteien sich mit diesem Thema im positiven Sinne beschäftigen würden. Wohl aber trifft es zu, dass die CDU/CSU sich mit dem Thema der Digitalisierung aller gesellschaftlichen Lebensbereiche befasst. Und sie tut vieles, um beim digitalen Grundrechtsschutz bzw. dessen Abbau die politische Hoheit zurückzugewinnen.

- Die Konkurrenten

In Bezug auf die „Digitalisierungspolitik" hatte kurzfristig die Piratenpartei die Buzzwords benannt: Bürgerrechte und Transparenz. Dass Datenschutz und Open Data in einem Konflikt stehen können, haben die Piraten zwar in der politischen Realität des Alltags gemerkt, eine einigermaßen konsistente einheitliche Antwort zu diesem Konflikt bleibt diese Partei aber schuldig, weil die zwei in der Partei vertretenen Digitalisierungskonzepte nicht vereinbar sind und eine Optimierung im Zielkonflikt auf einer intellektuell höheren Ebene nicht angestrebt wird; dies wird gesellschaftlich – von den Piraten – nicht mehr gefordert; dies würde auch die oft fundamentalistisch denkenden ProtagonistInnen beider Lager überfordern. Anders als der Konflikt zwischen den grünen Fundis und Realos, der in den 80er Jahren öffentlich ausgetragen wurde und historisch zu pragmatischen Ergebnissen führte, ist der Konflikt zwischen Bürgerrechtlern und Spackeria in der Piratenpartei weiter latent.

Die FDP versuchte und versucht weiterhin sich als Bürgerrechtspartei zu profilieren. Sie hat mit Burkhard Hirsch, Gerhard Baum und Sabine Leutheusser-Schnarrenberger im Hinblick auf ihr Datenschutzengagement glaubwürdige ProtagonistInnen. Doch besteht bei dieser Partei eine ähnlich unüberwindbare Kluft zwischen zwei Parteiflügeln wie bei den Piraten: Wirtschaftsliberalismus und Bürgerrechtspolitik kommen sich ins Gehege, wenn private Wirtschaftsunternehmen zur großen Gefahr für die Bürgerrechte werden. Eine Auseinandersetzung hierüber hat bei der FDP nicht stattgefunden. Die Partei hat noch ein weiteres Problem: Selbst wenn diese Auseinandersetzung geführt würde, würde sie die Öffentlichkeit wohl nicht mehr zur Kenntnis nehmen – ist doch die Partei zu unwichtig geworden.

Die Linken vertreten einen manchmal radikalen, aber konsequenten Bürgerrechtsansatz – auch im Hinblick auf digitale Bürgerrechte und den Datenschutz. Der Riss bei diesem Thema geht nicht durch die Partei, sondern durch deren Geschichte: Die Linken sind – und das ist historisch unbestritten – die politischen Erben des Sozialistischen Einheitspartei SED der DDR. Und diese vertrat nun alles andere als eine (digitale) Bürgerrechtspolitik. Anders als die Grünen bei der Kindersexdebatte, stellten sich die Linken bisher nicht diesem historischen Widerspruch und arbeiteten diesen auf. Dieses Defizit trägt dazu bei, dass es einem Bundespräsidenten möglich war, einen thüringischen Ministerpräsidenten fälschlich mit dem freiheitsnegierenden SED-Überwachungsstaat in Verbindung zu bringen.

Programmatisch am nächsten und glaubwürdigsten in Sachen Datenschutz und digitale Bürgerrechte dürften weiterhin Bündnis 90/Die Grünen sein. Sie haben nicht die Defizite der vorgenannten Parteien: Öffentliche Transparenz und individuelle Freiheiten sind für sie zwei Seiten einer Medaille. Es gibt in der Partei eine kapitalismus- und eine staatskritische Tradition. Diese macht es der Partei einfach, eine klare Kritik an privatwirtschaftlich ausgeübter digitaler Fremdbestimmung zu formulieren. Das Problem von Bündnis 90/Die Grünen ist allenfalls ihr inzwischen gewonnener politischer Pragmatismus, der in Regierungsverantwortung das Verdrängen bürgerrechtlicher Tugenden zur Folge haben kann, so wie dies z. B. in der rot-grünen Koalition nach 9/11 unter einem Innenminister Otto Schily der Fall war.

Pragmatismus ist auch das Problem der SPD. Dieser erlaubt es der aktuellen Regierungspartei nicht mehr, die klaren Positionen zu vertreten, die sie, z. B. in Hinblick auf die Snowden-Enthüllungen zu NSA und GCHQ, als Opposition vertrat. Es gibt in der SPD unzweifelhaft eine digital-bürgerrechtliche Basis. Das Hauptproblem der (digitalen) Bürgerrechte ist, dass diese nie zur Identität dieser Partei gehörten. Weder das klassische Klientel noch die Funktionäre können mit diesem Thema viel anfangen. Dies trägt dazu bei, dass in dieser Partei auch keine profilierten ProtagonistInnen in Sachen digitale Bürgerrechte aktiv sind. Dass dieses Thema viel mit der sozialen Frage zu tun hat, hat die Partei (noch) nicht realisiert.

- Die CDU

Kommen wir zur Union. Diese tat sich lange mit dem Datenschutz und sonstigen digitalen Bürgerrechten relativ leicht: „Datenschutz ist Täterschutz" war die zentrale Parole. Auch bzgl. des Datenschutzes in der Privatwirtschaft konnte man sich schnell darauf verständigen, dass es sich hierbei um ein fortschritts-, und wirtschaftshinderliches, gesellschaftspolitisch eher weiches Anliegen handelte, dem man keine größere Aufmerksamkeit widmen musste und das man bei Bedarf bekämpfen und diffamieren konnte.

Das Problem an der Beibehaltung dieser Position liegt weniger bei den politischen Gegnern als bei zwei anderen auf dem Parkett der politischen Meinungsbildung relevanten Mitspielern: Das sind zum einen die in Sachen digitaler Ungerechtigkeit und Bevormundung äußerst sensiblen Medien, die die öffentliche Meinung beeinflussen. Und da ist das Bundesverfassungsgericht, das digitale Grundrechte und insbesondere das Grundrecht auf Datenschutz zum Kernbestand unserer freiheitlich-demokratischen Verfassung erklärt hat. Als moderne Partei kann es sich die CDU/CSU nicht mehr leisten, insofern die öffentliche Meinung zu ignorieren. Sie kann es sich nicht leisten, wie noch bis in die 90er Jahre hinein, allein patriotische Partei zu sein; heute gehört auch ein gehörig Maß Verfassungspatriotismus dazu. Und insofern hat nicht mehr die CDU die Definitionsmacht, sondern das Verfassungsgericht.

Das ändert nichts an dem Umstand, dass die CDU/CSU kein ideologisch festes Verständnis zum Datenschutz hat. Digitale Bürgerrechte und der Datenschutz sind eine disponible Masse; es besteht hierzu ein taktisches Verhältnis, das Angela Merkel markant auf den Punkt brachte, als sie meinte, dass das Bespitzeln unter Freunden überhaupt nicht gehe, die unverbrüchliche Freundschaft zu den weiter spitzelnden USA aber nicht ansatzweise in Frage stellte.

Die Positionen der CDU/CSU sind derzeit von größter Relevanz. Die Union hat das Thema regierungspolitisch usurpiert. Während in der schwarz-gelben Koalition die FDP zur konservativen Datenschutzpolitik der CDU klare Contrapunkte setzen konnte und dies letztlich oft zu einem politischen Stillstand führte, etwa bei der Vorratsdatenspeicherung oder bei sonstigen Sicherheitsgesetzen, fällt es dem neuen Koalitionspartner der CDU, der SPD, erkennbar schwerer, klare Kante zu zeigen. Es muss jedoch anerkannt werden, dass Justizminister Heiko Maas etwa bei der Diskussion um die Vorratsdatenspeicherung eine ähnliche Funktion wahrnimmt wie zuvor der kleinere Koalitionspartner. Erfreulich scheint auch, dass an die Stelle der öffentlichen Grabenkämpfe eher eine öffentlich geführte Debatte über gemeinsame Lösungen geführt wird.

Doch sind die Möglichkeiten der SPD, die CDU-Politik zu beeinflussen, äußerst gering. Dies zeigte sich gleich nach dem Start der schwarz-roten Regierung bei der Auswahl der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Andrea Voßhoff. Das Bestimmungsrecht lag bei der CDU. Diese benannte eine nicht wieder in den Bundestag gewählte CDU-Politikerin, die auf dem Gebiet bisher weder Kenntnisse noch Engagement vorweisen konnte. Deren Bestimmung erfolgte ohne öffentliche Diskussion. Weder zur Wahl noch seitdem zur Amtsführung sind von der SPD öffentlich kritische Statements festzustellen, obgleich deren Amtsführung von Regierungshörigkeit und Untätigkeit gekennzeichnet ist. Nach einem Jahr hätte Voßhoff und die CDU die Möglichkeit gehabt, ohne Gesichtsverlust die Person in der Funktion auszutauschen, nachdem durch den Wechsel der CDU-Abgeordneten Katharina Reiche in die Wirtschaft Voßhoff in den Bundestag hätte nachrücken können. Doch sie zogen es vor, eine stromlinienförmige Datenschutzbeauftragte zu halten und den Bundestagssitz vakant zu lassen.

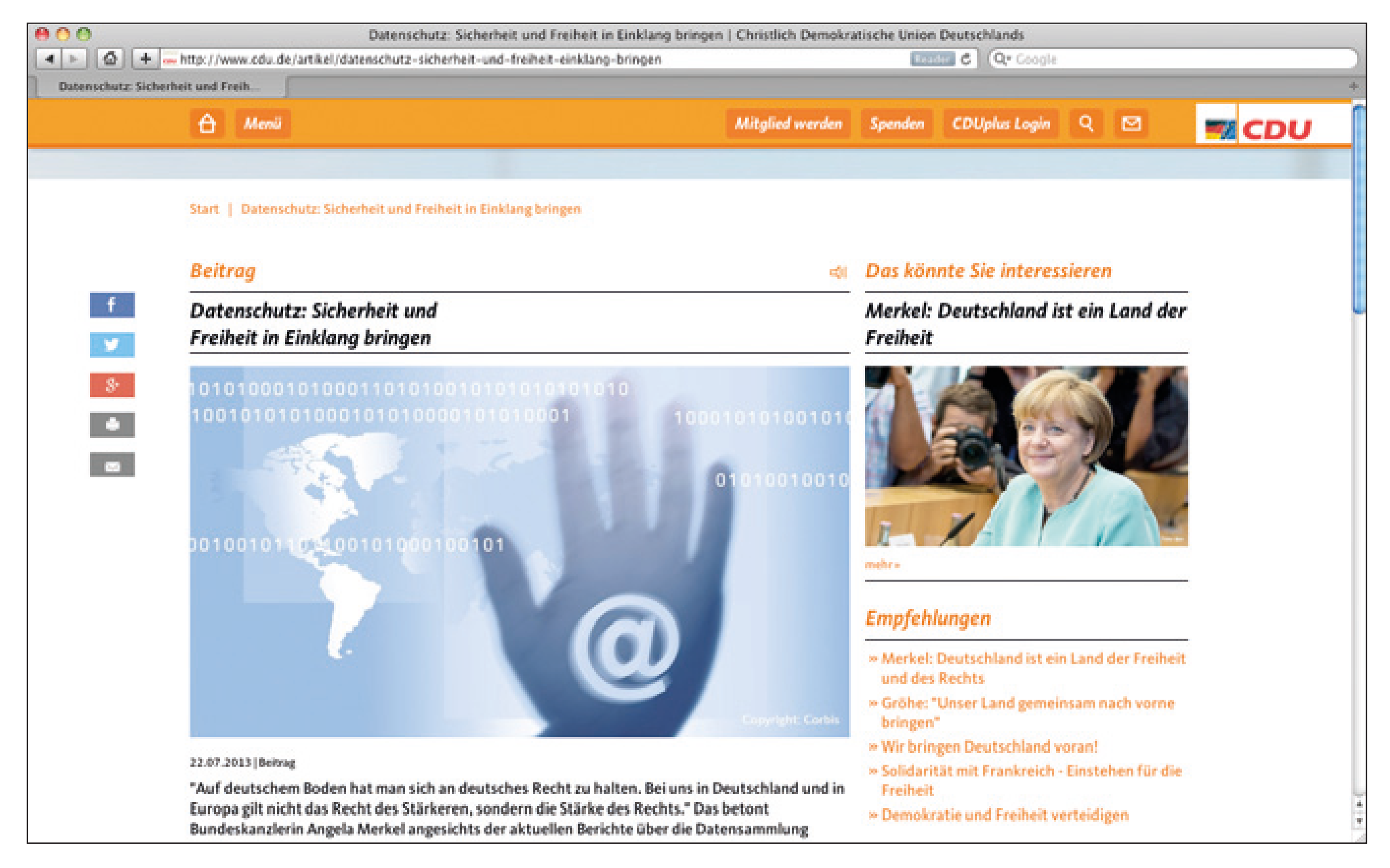
Gravierend für den digitalen Grundrechtsschutz ist weiterhin, dass in der Bundesregierung die CDU/CSU praktisch alle relevanten Ressorts mit eigenen Leuten besetzen konnte, das Ministerium für digitale Infrastruktur mit Alexander Dobrindt von der CSU und das in Fragen des Datenschutzes und der Sicherheitspolitik massiv dominierende Ministerium des Innern mit Thomas de Maizière. Das heißt: Ohne die CDU/CSU geht beim Datenschutz gar nichts. Heiko Maas hat als Justiz- und Verbraucherminister nur in kleinen Segmenten eigene Initiativmöglichkeiten; ansonsten bleibt ihm die Rolle, die zuvor Sabine Leutheusser-Schnarrenberger wahrnahm, nämlich das Schlimmste zu verhindern oder kleine Verbesserungen, wie die Einführung des Verbraucherverbandsklagerechts beim Datenschutz, zu bewirken. Wenn es dagegen um die „großen" Datenschutzthemen geht, etwa die Europäische Datenschutzgrundverordnung oder die Strukturen des nationalen Datenschutzrechtes, haben die unionsgeführten Ressorts das Sagen.

Ein Problem bei der Einschätzung der Unions-Politik besteht darin, dass es hierzu keine oder nur wenige aussagekräftige Statements gibt. Angesichts dieser Datenlage ist es nicht schädlich, im Folgenden einen der wenigen CDU-Politiker zu Wort kommen zu lassen, die die Digitalisierungspolitik der Union mit bestimmen, den Bundestagsabgeordneten Thomas Jarzombek:

- Statement Jarzombek

„Als Politik sind wir nicht der bessere Unternehmer, aber wir müssen einen ausgewogenen Rechtsrahmen zum Beispiel für den Datenschutz sicherstellen, der Innovationen ermöglicht. Der Wettbewerb in diesem Umfeld ist global, Deutschland begegnet diesem Umfeld mit einer Kleinstaaterei von 16 + 1 Datenschutzbeauftragten, deren Schwerpunkt augenscheinlich auf der Verhinderung von Datennutzung liegt. In politischen Diskussionen begegnet mir oft das Argument, der hohe deutsche Datenschutzstandard müsse Vorbild für Europa und damit Standortfaktor der Zukunft sein. Diese Argumentation hinkt – datenschutzfreundliche oder datensparsame Geschäftsmodelle und Angebote setzen sich auch in Deutschland nicht durch.

Die Debatte um den Datenschutz von Anwendungen bei Kurznachrichten-Apps hat der millionenfachen Nutzung in Deutschland nicht geschadet – obwohl es „sicherere" Produktalternativen gibt. Trotz strenger deutscher Datenschutzgesetze erleben wir eine Situation wie im Wilden Westen: Der Stärkere gewinnt. Ein vernünftiger Datenschutz muss zukünftig stärker differenzieren können zwischen sensiblen Daten und unkritischen Diensten. Dies muss sich auch in der Datenschutzgrundverordnung spiegeln, die keine Käseglocke für die europäische Internet-Wirtschaft werden darf. Das Datenschutzrecht ist entstanden als Abwehrrecht gegen den Staat, weil übermächtige Behörden persönliche Daten erfassten und sich der Bürger dagegen nicht wehren konnte. Es wäre eine Perversion dieser Gedanken, sollte künftig aufgrund zu strenger Opt-in-Regelungen aus Europa eine Situation entstehen, in der unbegrenzt alle persönlichen Daten gesammelt werden,



aber nur von den großen US-Playern, die immer ein Opt-in erhalten werden und dann Gatekeeper über diese Daten für europäische Gründer werden. Diese Gefahr scheint derzeit sehr real“ (zit. aus Netzpolitik? Es lebe die Digitalisierungspolitik, in DIVSI magazin, Dezember 2014, S. 7).

- Schlussfolgerungen

An der oben widergegebenen Position von Jarzombek ist zunächst einmal markant, dass „Digitalisierungspolitik“ ausschließlich als Wirtschaftspolitik und Innovationsförderung verstanden wird; die grundrechtliche Seite wird nicht einmal erwähnt, als Verbraucheraspekt erscheint lediglich die vermeintliche freie Entscheidung der KonsumentInnen, datenschutzwidrige Verfahren nutzen zu wollen. Zugleich taucht bei Jarzombek ein Argumentationsmuster auf, das unter Innenminister Hans-Peter Friedrich gepuscht wurde und letztlich das US-amerikanische Datenschutzverständnis propagiert: Die Abschaffung des Verbots mit Erlaubnisvorbehalt im nicht-öffentlichen Bereich und die Ablösung des Grundrechtsansatzes durch eine Risikobewertung, bei der nur noch sensible Datenverarbeitungen reguliert werden sollen – was auch immer man darunter verstehen mag. Dabei ist markant, dass Jarzombek etwas als Gefahr darstellt, was schon seit Jahren Realität ist: die US-Dominanz in Bereich der IT-Wirtschaft.

Diese wirtschaftsliberale Position wird nicht einmal vom wirtschaftsliberalen Flügel der FDP vertreten und widerspricht der insofern eindeutigen Rechtsprechung des Bundesverfassungsgerichtes und des Europäischen Gerichtshofes. Sie ignoriert zugleich die wirtschaftspolitische Chance für die europäische IT-Wirtschaft, nämlich mit dem ordnungspolitischen Instrument „Datenschutz“ die US-Anbieter ihren bisherigen rechtswidrig erlangten Wettbewerbsvorsprung streitig zu machen. Dass hierin eine reale Perspektive besteht, haben deutsche Unternehmen wie z. B. die Telekom erkannt, in einem gewissen Maße auch Branchenverbände wie der BITKOM und die Europäische Kommission. Von der Bundesregierung, speziell aus der Ecke von CDU/CSU, gibt es solche Statements bisher (noch) nicht.

Es ist zweifellos nicht einfach. Es muss aber angesichts der bestehenden politischen Lage in Deutschland ein zentrales Anliegen der Datenschutz-Szene sein, die CDU/CSU mit ihrer bisherigen Haltung zum Datenschutz und zu den digitalen Bürgerrechten zu stellen. Hierbei kann auf konservative Medien zurückgegriffen werden, die inhaltlich schon erheblich weiter sind als die PolitikerInnen der CDU/CSU und deren Bundesbeauftragte – allen voran die Frankfurter Allgemeine Zeitung, bis hin – zumindest partiell – zur Bild-Zeitung. Auf Veranstaltungen zum Datenschutz sollten CDU-PolitikerInnen eingeladen werden und zu klaren Stellungnahmen aufgefordert sein. Die CDU/CSU unter Angela Merkel und Horst Seehofer hört insbesondere auf eine – des Volkes – Stimme bzw. wie sie wahrgenommen wird. Zur Stimme des Volkes gehören für die CDU/CSU – mehr als für andere Parteien – auch die christlichen Kirchen, die bisher zu den digitalen Herausforderungen in unserer Gesellschaft sehr still sind. Die CDU fühlt sich beim Thema digitale Grundrechte völlig unbelastet von der Geschichte, von Ideologien oder von Parteiflügeln. Es besteht also eine Chance und die Notwendigkeit, sie – nicht nur über die ökonomischen Chancen, sondern auch – mit der bürgerrechtlichen und der demokratischen Komponente anzusprechen.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

„Freiwillige" Gesundheitsdaten bald bei Versicherer Generali?

I. Das angekündigte Angebot

November 2014 wurde bekannt, dass die Generali-Versicherungsgruppe als erstes großes Unternehmen in Europa auf elektronische Kontrolle von Fitness, Lebensstil und Ernährung setzt und dabei mit dem südafrikanischen Versicherer Discovery kooperiert. Discovery hat das Gesundheitsprogramm „Vitality" entwickelt, das KundInnen mit Gutscheinen, Geschenken und Rabatten belohnt, wenn sie sich gesund verhalten und dies nachgewiesen wird. Danach werden Generali regelmäßig Daten zum Lebensstil übermittelt mittels einer App, die Vorsorgetermine dokumentiert, Schritte zählt oder sportliche Aktivitäten misst. Auch gesunde Ernährung gehört zum Paket, so Generali-Konzernchef Mario Greco vor Investoren: „Damit stärken wir die Bindung zu unseren Kunden. Außerdem beeinflussen wir das Verhalten unserer Kunden, und gesündere Kunden sind besser für uns." In einer ersten Stufe sollen die Versicherten, die sich gesundheitsbewusst verhalten, Gutscheine für Reisen und das Fitnessstudio bekommen. Im nächsten Schritt seien Prämiennachlässe beim Versichertenschutz möglich. Generali kündigte an, diese Angebote in 12 bis 18 Monaten auch in Deutschland bereitzustellen.

Das Verfahren ist vergleichbar mit der Kontrolle des Autofahrens und dem Berücksichtigen der Ergebnisse bei der Preisfindung für die Kfz-Versicherung. In Deutschland ist die Resonanz hierfür schwach, in Italien und Großbritannien dagegen sehr hoch. Nicht nur Generali, auch Allianz, AXA und andere Versicherer arbeiten an solchen Projekten. Sie versprechen KundInnen, bei einer gesünderen Lebensweise zu helfen. Alle Unternehmen betonen, die Daten nur zu verwenden, die Versicherte ihnen freiwillig geben. Doch wollen sie mit den Daten ihr Klientel so genau wie möglich kennenlernen, um einen individuellen Tarif anzubieten. Dies bedeutet auch, dass derjenige mehr bezahlt, der risikoreicher lebt. Und wer nicht bereit ist, seine Daten preiszugeben, läuft Gefahr, einen deutlich höheren Preis für seine Versicherung zu bezahlen. Einer der Vorreiter ist der US-amerikanische Krankenversicherer United Healthcare. Er bietet Kunden schon seit drei Jahren einen Preisnachlass an, wenn sie täglich eine bestimmte Anzahl von Schritten tun und dies nachweisen können.

II. Kritische Reaktionen

Die Reaktion von Verbraucherschützern auf die Generali-Ankündigungen waren wenig begeistert, etwa Peter Grieble von der Verbraucherzentrale Baden-Württemberg: „Der Kunde weiß ja gar nicht, wie seine Daten im Konzern verarbeitet werden und wer Zugriff darauf hat." Könne jeder Sachbearbeiter Informationen zum Gesundheitszustand oder zur Fahrweise abrufen, sei das problematisch. Doch wüssten private Krankenversicherungen schon heute alles über den Gesundheitszustand, was an Arztrechnungen und Rezepten eingereicht worden ist.

Auch Datenschutzbeauftragte äußerten sich kritisch, etwa Reinhardt Dankert aus Mecklenburg-Vorpommern: „Ich rate aus mehreren Gründen dazu, solche Angebote links liegen zu lassen. Wenn überhaupt, kann man diese Entwicklung nur noch über den Markt und evtl. noch durch längst überfällige rechtliche Grenzen aufhalten." Mit solchen Instrumenten werde die Ökonomisierung unserer Lebensdaten betrieben: „Unternehmen, die ihre Kunden auf der Grundlage des Wahrscheinlichkeitsdenkens nach dem Risikoäquivalenzprinzip einteilen, befördern auf diese Weise Solidaritätsbrüche, die in einer schonungslosen Individualisierung enden werden. In einem Gemeinwesen, in dem das möglichst lückenlose Datensammeln in sensiblen Bereichen wie Gesundheit, Arbeit, Engagement und Konsum üblich ist, werden diejenigen zu ´Bestraften`, die sich dieser Sammlung entziehen oder schlicht nicht normgerechte Werte liefern. Diese immer umfassendere Datentransparenz wird die Geister nicht mehr los, die sie gerufen hat. Wer sich auf das Spiel des Perfektionismus eingelassen hat, wird also primär perfekt zu sein haben und jede Information, die nicht verfügbar ist, hält ihn von dieser – notwendigen – Perfektion ab." Ihn ergänzt der Datenschutzbeauftragte von Nordrhein-Westfalen Ulrich Lepper: „Persönlichste Daten zur täglichen Lebensführung sollten Versicherungen nicht zur Verfügung gestellt werden, nur um einen Preisvorteil zu erhalten. Mit solchen Geschäftsmodellen wird ein finanzieller Druck erzeugt, tiefen Einblick in Lebensgewohnheiten und Gesundheit zu ermöglichen. Es ist Zeit für eine gesellschaftliche Debatte, wo Grenzen für solche Geschäftsmodelle zu ziehen sind."

Das Thema wurde von der Schriftstellerin Juli Zeh in ihrem dystopischen Roman „Corpus Delicti" aus dem Jahr 2009 verarbeitet. Anlässlich der Generali-Pläne meinte sie: „Das Streben nach Sicherheit, Gesundheit, Schmerz- und Risikofreiheit führt letztlich zu einem totalitären Gesellschaftsmodell. Wir folgen derzeit dem Irrglauben, unser Schicksal, sprich unsere Zukunft beherrschen zu können, indem wir ständig alles ‚richtig' machen und uns unentwegt selbst optimieren – in der Arbeit, bei Gesundheit und Ernährung, selbst bei Liebe und Sex. Alles ist Leistungssport. Wir glauben, dadurch Kontrolle über unser

Leben zu gewinnen. In Wahrheit werden wir manipulierbar und unfrei. Im 20. Jahrhundert gingen Unterdrückung und diktatorische Methoden von Staaten aus. Inzwischen erleben wir, wie große Konzerne immer mehr Macht gewinnen, sich zum Teil gar nicht mehr an Politik und Gesetze gebunden fühlen. Totalitäre Strukturen kleiden sich heute im Gewand von Serviceangeboten. Es ist die Aufgabe der Politik, das Individuum davor zu schützen, zum Objekt von Interessen zu werden." Es drohe eine Entsolidarisierung in der Gesellschaft: „Längst verlieren die meisten Menschen den Sinn für Solidarität. Sie fragen: ‚Warum soll ich für den Bluthochdruck von dem fetten Kerl da aufkommen? Soll der doch weniger essen!' Die Leute fangen an zu vergessen, dass persönliche Freiheit nicht aus individueller Höchstleistung resultiert, sondern aus gesellschaftlichem Zusammenstehen. Denn Freiheit braucht Absicherung, und die gibt es nur durch Solidarität. Der Selber-schuld-Gedanke macht uns alle unfrei.

Das Problem der individualisierten Tarife besteht darin, dass sie das Versicherungsprinzip ad absurdum führen: Versicherer gleichen mit ihrem Angebot dank der großen Zahl und der langen Geltungsdauer verschiedene Risiken und die dabei entstandenen Schäden aus. Mit den individualisierten Tarifen versuchen die Unternehmen nun, die „besten Risiken" für sich zu gewinnen und die „schlechten Risiken" an die Konkurrenz wegzudrücken. Trotz der Preisnachlässe kann so mehr Gewinn gemacht werden. Felix Hufeld von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sieht dies kritisch: „Wenn wir den Gedanken zu Ende denken, kann das letztlich zu einer Atomisierung des Kollektivs führen."

Der Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) erklärt das „Gesetz der großen Zahl" wie folgt: „Je mehr, desto besser: Wer in eine Versicherung einzahlt, bekommt im Schadensfall einen finanziellen Ausgleich – und zwar in aller Regel deutlich mehr, als er eingezahlt hat. Dass Versicherungen trotzdem erfolgreich agieren, liegt daran, dass viele Menschen bei ihnen versichert sind und nicht bei allen ein Schaden eintritt. Der Risikoausgleich im Kollektiv reduziert also das Zufallsrisiko für den Kunden. Eine hohe finanzielle Belastung, die zu einem unbekannten Zeitpunkt fällig werden kann, wird ersetzt durch eine planbare Beitragszahlung. Der mathematische Hintergrund, um diese Versicherungsrisiken zu berechnen, ist das Gesetz der großen Zahl – ein Grundsatz der Wahrscheinlichkeitsrechnung. Es besagt, dass sich mit der wachsenden Zahl von gleichartigen zufälligen Ereignissen die daraus resultierenden Ergebnisse immer genauer vorhersagen lassen. Versicherungsunternehmen versuchen entsprechend, möglichst viele Kunden für den gleichen Schadensfall zu versichern. Im Einzelfall kommen auch Rückversicherer zum Einsatz, um eine ausreichend hohe Zahl zu erreichen."

III. Relativierungen von Generali, aber kein Dementi

Die heftige öffentliche Reaktion auf die Generali-Ankündigung veranlasste Christoph Schmallenbach, Vorstand der deutschen Generali, vorsichtig zurückzurudern: „Unser Konzern fragt nicht nach dem Sexualleben seiner Kunden und wird es auch in Zukunft nicht tun. Es geht um ein komplettes Gesundheits- und Fitnessprogramm. ´Vitality` ist ein Angebot, Jungen und Alten, Gesunden und Kranken dabei zu helfen, gesünder zu leben. Wenn der Kunde gesundheitsbewusster leben will, kann er diese und jene Stellhebel bewegen. Das ist die Idee. Die konkrete Ausprägung ist dann länderspezifisch. Das Erstaunliche an der Diskussion ist: Es gibt noch nichts Konkretes. Für Deutschland erarbeiten wir ein solches Angebot erst. Es wird auf jeden Fall ein Angebot sein, das auf die deutschen Verhältnisse zugeschnitten ist, zu unseren strengen Datenschutzvorschriften und zu unseren Vorstellungen von Privatsphäre passt. Der Kunde entscheidet allein, ob er diese Sorte Produkt haben will und was überwacht wird. Das hat mit Orwell nichts zu tun.

Ich sehe nicht, dass wir uns irgendwann mit der Genanalyse beschäftigen. Eine Genanalyse ginge definitiv zu weit. Bei uns hat das Kundenvertrauen absolute Priorität. Wir wollen ja gerade dafür sorgen, dass die Situation für den Kunden beherrschbar bleibt. Die Daten sind nützlich für Kunde und Versicherer. Versicherungen sind nun mal ein datenintensives Geschäft" (Gröger, Der elektronische Patient, SZ 21.11.2014, 17; LDI Nordrhein-Westfalen, PE 21.11.2014, Kein Ausverkauf von Gesundheitsdaten; LfDI Mecklenburg-Vorpommern, PE 02.12.2014, Fitness-Apps für Krankenkassen – der nächste Schritt zur Entmündigung 2.0; Interview Janker mit Zeh: „Wir werden manipulierbar und unfrei", SZ 25.11.2014, 26; Interview Brauch/Hawranek mit Schmallenbach, „Wir fragen nicht nach Sex", Der Spiegel 50/2014, 88 f.; GDV, Kurz erklärt – Gesetz der großen Zahl, Positionen Nr. 95 (2014), S. 31).

Bund

Dienste liefern weiter US-Behörden Dschihadisten-Daten

Aller Kritik an der US-Spionage in Deutschland zum Trotz teilen deutsche Sicherheitsbehörden offenbar noch immer heikle Personendaten mit den USA. Im Jahr 2014 soll Deutschland detailliert Auskunft gegeben haben über Hunderte junge Männer, die sich in Syrien und im Irak der Terrormiliz Islamischer Staat (IS) anschließen wollten. Bei den Verdächtigen soll es sich um deutsche Staatsbürger handeln und um Ausländer mit Aufenthaltserlaubnis in der Bundesrepublik. Übermittelt wurden demnach an die US-Dienste umfangreiche persönliche Datensätze einschließlich Namen, Telefonnummern und E-Mail-Adressen.

Dem Pressebericht aus den USA zufolge hatten die deutschen Behörden Bedenken, die persönlichen Daten zu erheben und mit einem Verbündeten zu teilen. Doch erhofften sie sich von der Kooperation Hilfe beim Versuch, die Spuren der Dschihadisten zu verfolgen, um sie nach deren Rückkehr beobachten zu können. Sicherheitsbehörden in vielen westlichen Ländern sind besorgt, dass Kämpfer des IS nach der Rückkehr Terroranschläge planen. Der UN-Sicherheitsrat hat im Herbst eine Resolution verabschiedet, die alle Länder zur Kooperation gegen „ausländische Kämpfer" auffordert. Ein zitierter hochrangiger deutscher Sicherheitsbeamter

vergleicht das Verhältnis zu den USA mit einer Ehe, in der die Partner eigentlich das Vertrauen ineinander verloren haben; eine Scheidung sei aber keine Option (Richter, Deutschland lieferte Daten, SZ 31.12.2014, 6).

Bund

Telekommunikationsunternehmen MCI ließ BND mithören

Die deutsche Tochter des US-Providers MCI mit Sitz in Dortmund soll dem Bundesnachrichtendienst (BND) Zugang zu ihren Telefonleitungen verschafft haben. Der Mutterkonzern MCI war bis zu seiner Übernahme durch Verizon im Jahr 2006 eines der größten Telekommunikationsunternehmen der Welt. Das Unternehmen war aus der Übernahme von MCI Communications durch Worldcom hervorgegangen. Worldcom hatte nach Bilanzmanipulationen im Juli 2002 Gläubigerschutz beantragt.

Vor dem Untersuchungsausschuss des Bundestags hatte der BND-Projektleiter bereits im November 2014 über eine Kooperation des BND mit dem US-amerikanischen Dienst NSA unter dem Codenamen „Eikonal" berichtet, wonach der BND 2003 bis 2008 für die US-Amerikaner an einem Telekom-Datenknoten in Frankfurt massenhaft Daten abfischte und auf bestimmte Schlagworte hin selektierte und die Ergebnisse dieser Auslandsverkehre – jährlich mehrere Hundert Mitteilungen – dem US-Geheimdienst CIA zur Verfügung stellte. Bei seiner Aussage in geheimer Sitzung soll der BND-Projektleiter allerdings zunächst einen falschen amerikanischen Provider genannt haben. Das Nachrichtenmagazin „Der Spiegel" räumte ein, einen falschen Namen der Operation genannt zu haben. Anders als zunächst berichtet, laute er nicht „Globe", sondern „Glotaic", wobei die letzten drei Buchstaben für die CIA stünden. Die Verwirrung könnte auch daher rühren, dass der Name in den Unterlagen für den NSA-Ausschuss zum Teil geschwärzt war. Nach Aussagen von Ausschussmitgliedern waren nur die ersten drei Buchstaben „Glo" zu erkennen. Die Linke-Ausschussobfrau Martina Renner kündigte am 17.01.2015 an, der Ausschuss werde sich mit der Operation Glotaic „nach Eikonal (Abgreifen von Kommunikationsdaten bei Telekom) beschäftigen".

Dem ursprünglichen Bericht zufolge wurden Daten von dem Netzbetreiber in die BND-Außenstelle Rheinhausen geleitet und dort aufbereitet. Damals trug die Dienststelle noch den Decknamen Ionosphäreninstitut. Es soll sich um eine zeitlich befristete Operation mit dem Schwerpunkt Terrorismusabwehr gehandelt haben. Es sollen ausschließlich Auslandstelefonverkehre, etwa von Afghanistan nach Pakistan, abgefangen worden sein. Die Telekommunikationsanbieter sind gesetzlich nicht verpflichtet, dem BND in Deutschland Zugriff auf ausländische Kommunikationsdaten zu gewähren. Um Bedenken der Deutschen Telekom für die Operation Eikonal auszuräumen, hatte sich sogar das Bundeskanzleramt eingeschaltet. MCI soll ebenfalls nicht zu einer sofortigen Kooperation bereit gewesen sein und Rücksprache mit seinem amerikanischen Mutterkonzern gehalten haben. Schließlich habe man sich auf eine Zusammenarbeit unter Einbindung der CIA geeinigt (US-Telefonriese ließ BND mithören, Der Spiegel 3/2015, 13; Denkler, Der Apotheker vom BND, SZ 05.12.2014, 6; BND erhielt Daten offenbar von MCI, www.golem.de 10.01.2015).

Bund

Bahn treibt Videokontrolle voran

Die Deutsche Bahn AG will mit mehr Videoüberwachung für Sicherheit auf Bahnhöfen sorgen. Das Bundesunternehmen kündigte kurz vor Jahreswechsel an, im Jahr 2015 bis zu 700 Kameras auf rund 100 Stationen anzubringen und die Aufzeichnungen bis zu drei Tage zu speichern. Welche Bahnhöfe genau betroffen sind, will das Unternehmen noch festlegen. Die Bundespolizei könnte dann auf 240 der knapp 5400 Bahnhöfe die Bahnkameras mitnutzen. Bahn und Bundesinnenministerium hatten im Sommer 2013 vereinbart, bis 2019 gemeinsam 36 Millionen Euro zu investieren, um die Videoüberwachung zu modernisieren und auszubauen. Weitere 24 Millionen Euro sollen in die sogenannten 3-S-Zentralen der Bahn für Sicherheit, Sauberkeit und Service fließen. Von den Gesamtkosten von 60 Millionen Euro übernimmt 15 Millionen Euro die Bundespolizei. Die nun angekündigten weiteren 700 Kameras installiert die Bahn zusätzlich und auf eigene Rechnung.

Gerd Becht, der im Bahnvorstand für die Bereiche Recht und Konzernsicherheit zuständig ist, meinte: „Damit wollen wir die Polizei bei der Bekämpfung von Straftaten schnell und unkompliziert unterstützen. Die Sicherheit unserer Kunden steht für uns im Mittelpunkt." Derzeit hängen nach seinen Angaben 4.800 Kameras in 640 Bahnhöfen. Auf 140 Stationen davon würden die Aufzeichnungen gespeichert. Weitere 18.000 Videokameras gebe es in Regional- und S-Bahn-Zügen, so dass 80% der Fahrgastströme gefilmt werden, wie die Bahn errechnet hat.

Bahnhöfe und Züge sind vergleichsweise sichere Orte, um sich aufzuhalten. So transportiert die Bahn täglich mehr als 7,3 Millionen Menschen, das ist doppelt so viel, wie in Berlin wohnen. Bei der Bahn kommt es täglich bundesweit zu 40 Körperverletzungen, während sich in Berlin im Schnitt sechs Mal mehr ereignen. Die Videoüberwachung an Bahnhöfen wurde 2012 ein großes Thema, nachdem am Bonner Hauptbahnhof ein Bombenattentat missglückt war. Es hatte sich herausgestellt, dass die Bahn den Tatort zwar überwacht, aber keine Bilder aufgezeichnet hatte. Da die Aufzeichnung nicht der Sicherheit des laufenden Betriebs diene, sondern der Bekämpfung von Kriminalität, war dafür die Bundespolizei zuständig.

Positiv zu den Plänen äußerte sich der stellvertretende Vorsitzende der Gewerkschaft der Polizei, Jörg Radek: „Ein Mehr an Videoüberwachung sorgt auch für ein Mehr an Sicherheit." Überwacht würden vor allem große Bahnhöfe, weil dort die meisten Fahrgäste unterwegs seien. Fahrgastvertreter fordern immer wieder, auch kleinere Bahnhöfe besser zu überwachen; nach Umfragen fühlt sich jeder vierte Fahrgast an Bahnhöfen und Haltestellen in Deutschland unsi-

cher. Dafür seien aber mehr Polizisten nötig, sagte Radek. „Die Bundespolizei muss personell so ausgestattet sein, dass wir auch dort präsent sind, wo wir Videolücken haben."

Kritiker der Videoüberwachung monieren, sie spiegle eine scheinbare Sicherheit vor und greife tief in Persönlichkeitsrechte ein. Präventiv könnten Übergriffe durch Kameras nicht verhindert werden. Auch repressiv gebe es viele Möglichkeiten, sich einer Identifizierung zu entziehen. Während an sicherheitsrelevanten Plätzen, etwa bei der Zugabfertigung an den Gleisen oder vor Schließfächern, eine Überwachung akzeptiert werden könne, müssten allgemeine Räume, wo sich Menschen aufhalten und treffen, überwachungsfrei bleiben. Die undifferenzierte Forderung nach mehr Videoüberwachung tendiere zur Totalkontrolle. Auch die Bahn hatte noch vor zwei Jahren zu Bedenken gegeben, Kameras könnten zwar bei der Aufklärung helfen, seien aber kein geeignetes Mittel, um Straftaten zu verhindern. So schreckten die Kameras Betrunkene oder Menschen, die im Affekt handelten, nicht ab (Kuhr, Bahn verstärkt Videokontrolle an Bahnhöfen, www.sueddeutsche.de 22.12.2014, Bahn treibt Videokontrolle voran, www.abendzeitung-muenchen.de 22.12.2014).

Bund

Weiterhin großes Interesse an Stasi-Akten

Auch 25 Jahre nach dem Mauerfall wollen Menschen noch wissen, was die Stasi über sie gesammelt hat. Im Jahr 2014 gingen bis Anfang Dezember mehr als 61.000 Anträge in der vom Bundesbeauftragten für die Stasi-Unterlagen Roland Jahn geleiteten Stasi-Unterlagen-Behörde ein. Jeder einzelne wird gründlich geprüft, was teilweise lange dauert: „Wir unternehmen große Anstrengungen, die Akten zur Verfügung zu stellen. Doch wir schieben eine Bugwelle vor uns her." 2013 wurde knapp 64.250 Mal persönliche Akteneinsicht beantragt, 2012 waren es noch rund 88.200 Anträge gewesen. Die Stasi-Unterlagen-Behörde kämpft seit langem gegen die Wartezeiten. Die sind laut Jahn auch eine Folge der Personalplanung der Behörde, die von Anfang an mit sinkenden Mitarbeiterzahlen konzipiert worden sei. „Damit hat keiner gerechnet, dass mehr als zwei Jahrzehnte nach dem Mauerfall jeden Monat noch Tausende neue Anträge kommen." Derzeit hat die Behörde samt Außenstellen knapp 1.600 Mitarbeiter, 2003 waren es noch rund 2.300. Die Auskunftsabteilung wurde laut Jahn zwar verstärkt, doch das reiche nicht. „Wir brauchen Reformen. Die Mitarbeiter müssen für die Bürger da sein können."

Menschen, zu denen es nur wenige Quellen gibt, bekämen innerhalb von vier, fünf Monaten Auskunft, sagte Jahn. „Wenn viel Material da ist, dauert es länger." Rehabilitierungsersuchen sowie Anträge von Älteren und Kranken würden vorgezogen. Auch für Behörden, Forscher und Medien werde nach Stasi-Papieren gesucht. 2014 beantragten rund 37.000 Menschen das erste Mal die persönliche Akteneinsicht mit unterschiedlichen Gründen. Neu-Rentner haben nun Zeit und wollten ihr Leben ordnen. Verstärkt fragen in Familien Kinder und Enkel nach der Vergangenheit (Interesse an Stasi-Akten ist ungebrochen, www.n-tv.de 26.12.2014).

Bundesweit

Mitarbeiter-Screening mit Terrorlisten

Der Autokonzern Daimler überprüft seit Dezember 2014 alle drei Monate, ob Mitarbeitende auf Terror-Sanktionslisten stehen. Auch andere Firmen tun dies bereits oder planen es zu tun. Betroffen sind bei Daimler mit Stammsitz in Stuttgart etwa 280 000 Mitarbeitende. Am 12.11.2014 wurde in einer Konzernbetriebsvereinbarung festgelegt, dass die Stammdaten – Name, Anschrift und Geburtsdatum – aller Beschäftigten mit Sanktionslisten der Europäischen Union (EU) und der USA abgeglichen werden. Betroffen sind auch Personen, die sich bei Daimler bewerben. Das Unternehmen erklärte, dass der Abgleich auch in Bezug auf die leitenden Angestellten durchgeführt wird, wenngleich diese von der Betriebsvereinbarung nicht mit erfasst werden. Gibt es beim Abgleich einen „Treffer", so soll eine erneute Prüfung erfolgen. In anderen Unternehmen sei dies nicht der Fall. Bleibe es bei dem Verdacht, werde der Mitarbeiter freigestellt, das Entgelt werde nicht bezahlt und auf ein Treuhandkonto überwiesen. Der Mitarbeiter werde angehört und der Konzern berate ihn auch dabei, wie er von der Liste herunterkommen kann.

Daimler-Rechtsvorstand Christine Hohmann-Dennhardt erklärte, man sei sich der „Verantwortung bewusst" und werde mit den Daten sorgfältig umgehen. Eine Konzernsprecherin betonte, dass Daimler damit EU-Vorgaben umsetze. Die EU sowie die USA haben zwingende Gesetze zur Durchsetzung von Embargos und zur Terrorismusbekämpfung sowie entsprechende strikt zu beachtende Sanktionslisten (EG-VO 2580/2001, EG-VO 881/2002 und EU-VO 753/2011) erlassen. Personen, die auf diesen Listen stehen, dürften weder Gelder noch Produkte oder Dienstleistungen erhalten. Alle Unternehmen seien verpflichtet, diesen Anforderungen nachzukommen und sicherzustellen, dass diese innerhalb ihres Verantwortungsbereichs eingehalten werden. Im Leitfaden „Antiterrorgesetzgebung" des Arbeitgeberverbands BDA heißt es: „In den Verordnungen wird nicht auf die Frage eingegangen, was konkret zu unternehmen ist". Dessen ungeachtet kann die Nichteinhaltung dieser gesetzlichen Vorgaben zu strafrechtlichen Konsequenzen für das Unternehmen führen. Die Vertraulichkeit aller Mitarbeiterdaten ist nach Angaben der Daimler-Sprecherin dadurch gewährleistet, dass der Abgleich durch eine kleine Gruppe innerhalb der Personalabteilung erfolge. Daimler wolle sich nicht, wie andere Unternehmen, auf die Banken verlassen, die ja auch zum Datenabgleich verpflichtet sind. „Die haben uns nicht schriftlich geben wollen, dass sie den Datenabgleich machen. Und es ist in Deutschland doch auch so: Das Gehalt muss nicht unbedingt auf das Konto des Arbeitnehmers gehen, das kann ja auch ein anderes Konto sein, aber wir stehen in der Verantwortung und haften für Fahrlässigkeit."

Daimler hat Erfahrungen mit dem Datenabgleich: Sermet I. war als Kind türkischer Eltern in Sindelfingen gebo-

ren und arbeitete als Lackierer bei Mercedes. Während einer Auszeit 2006 besorgte Sermet I. der islamischen Terrorgruppe Al Qaida Entfernungsmess- und Nachtsichtgeräte, flog auf und wurde verurteilt. Im Jahr 2012 wollte er sich wieder einklagen. Das Arbeitsgericht stellte jedoch fest, dass dies Daimler nicht zumutbar sei.

Die Gewerkschaften halten sich mit Kritik zurück, weil sie sich rechtlichen Zwängen gegenübersehen, auf die sie keinen Einfluss haben. Die Betriebsräte vor Ort müssten hier gestaltend wirken, ein Anrecht darauf haben sie allerdings nicht, das Screening sei nicht mitbestimmungspflichtig. Bereits 2011 hat die IG Metall Modell-Betriebsvereinbarungen für den Datenabgleich ausgearbeitet. In einem Statement erklärte die Gewerkschaft zur Entwicklung bei Daimler: „Die IG Metall nimmt zur Kenntnis, dass global tätige Konzerne weltweiten Rahmenbedingungen unterliegen. Dazu gehört u. a. der Abgleich von Terrorlisten mit Personendaten. Das hat Auswirkungen auf Beschäftigte und ihre persönlichen Daten. Der Schutz dieser Arbeitnehmerdaten ist für die IG Metall ein hohes Gut.“ Die Beschäftigten müssten vor falschen Verdächtigungen und dem damit einhergehenden „sozialen Tod im Netz“ geschützt werden. Dazu diene auch ein Abgleich der Daten unter Einbezug des Datenschutzbeauftragten, wovon der Betriebsrat regelmäßig in Kenntnis zu setzen sei. Im Falle eines falschen Verdachts müsse das Unternehmen eine schnelle Rehabilitation bewirken. „Die IG Metall begrüßt, dass der Betriebsrat von Daimler diese Punkte mit einer Betriebsvereinbarung umgesetzt und seine Mitbestimmungsrechte wahrgenommen hat.“ In wie vielen Betrieben der Datenabgleich erfolgt oder es eine Betriebsvereinbarung gibt, konnte die IG Metall nicht sagen, so eine Sprecherin: „Aber eigentlich betrifft das Thema ja jedes Unternehmen, das im Exportgeschäft tätig ist.“ Der Betriebsrats-Vorsitzende von Daimler Jörg Spiess erklärte die Betriebsvereinbarung zu einem „Leuchtturm zum Schutz der Beschäftigten“. Es könne kein Zweifel daran bestehen, dass Gesetze und Vorschriften eingehalten werden.

Andere Unternehmen überprüfen in vergleichbarer Weise die Daten der Mitarbeitenden. Auch Ford hat dazu eine Betriebsvereinbarung abgeschlossen. Wer auffällt, wird an das Bundesamt für Wirtschaft und Ausfuhrkontrolle gemeldet. Siemens gleicht ohne Betriebsvereinbarung ab, wie ein Sprecher erklärt: „EU- und US-Verordnungen enthalten Sanktionsbestimmungen, dass auf sogenannten Terror- bzw. Sanktionslisten aufgeführte Personen und Organisationen weder direkt noch indirekt Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden dürfen. Bei Siemens erfolgt vor jeder Gehaltszahlung ein Abgleich der Mitarbeiter/innen gegen diese Listen der europäischen und US-Behörden. Bereits bei der Einstellung eines Mitarbeiters erfolgt eine entsprechende Prüfung gemäß dieser Regelungen.“ Der Essener Stahl- und Industriegüterkonzern Thyssen-Krupp screent nur einen Teil seiner Beschäftigten, nämlich die im Kriegsschiffbau tätig sind. Aus Sicht dieses Konzerns sehe die Anti-Terror-Verordnungen der EU keine Verpflichtung vor, alle Beschäftigte zu überprüfen. Außerdem erfolge bei den Banken anlässlich der Gehaltsüberweisungen ein Abgleich. Auch alle Geschäftspartner und Kunden des Ruhrkonzerns werden mit den Terrorlisten abgeglichen. BMW und Volkswagen (VW) verzichten völlig auf eigene Maßnahmen und setzen ganz auf den Bankenabgleich. Die Airbus Group, die eine große Verteidigungs- und Militärsparte hat, überprüft neue Mitarbeitende. Um in besonders sensible Bereiche zu kommen, müssen sich die Mitarbeitenden zusätzlich vom Bundesinnenministerium durchleuchten lassen.

Datenschützern ist das Screening in vielen Punkten ein Dorn im Auge, vor allem der Abgleich mit US-Listen, die auch in die EU-Listen einfließen. Auf der Internet-Seite anwaltauskunft.de wird darauf hingewiesen, dass sich Terrorverdächtigte wegen hoher Hürden nur schwer zur Wehr setzen können: „Steht jemand etwa unberechtigterweise auf einer EU-Terrorliste, bleibt ihm einzig die Option, sich an den Europäischen Gerichtshof zu wenden“ (Bialdiga/Flottau/Fromm/Giesen/Hägler, Auf Verdacht, SZ 17./18.01.2015, 26; Burger, Firmen setzen auf Mitarbeiter-Screening, www.vdi-nachrichten.com 16.01.2014; Daimler durchleuchtet Mitarbeiter, Der Spiegel 2/2015, 57; vgl. DANA 4/2013, 165).

Bayern

Schulen missachten Videovorschriften

An mehr als der Hälfte der befragten Schulen, die mit Kameras überwachen, fehlten bei journalistischen Recherchen die erforderlichen Hinweisschilder. Bei der Befragung von 20 Schulleitungen konnten die meisten keine Vorfälle wie Gewalt oder Vandalismus nennen, die den Einsatz von Überwachungskameras rechtfertigen würden. Insgesamt sind nach Angaben des Innenministeriums an 172 bayerischen Schulen Videokameras installiert. Der Landesbeauftragte für Datenschutz, Thomas Petri, kündigte eine „krachende Beanstandung“ für die Schulen an; die recherchierten Fälle würden an die Aufsichtsbehörde weitergeleitet: „Die Schulleitung kann sich warm anziehen“, denn Tonaufzeichnungen oder heimliche Aufnahmen seien verboten.

Der Sprecher des Kultusministeriums Ludwig Unger betonte dagegen, dass er von der Einhaltung der Datenschutzregeln an den Schulen ausgehe. „Wenn uns Hinweise auf Verstöße gegen den Datenschutz vorliegen, werden wir dem nachgehen.“ Für jede Schule müsse es ein Sicherheitskonzept geben, das mit der Polizei abgestimmt werde. Für bauliche Maßnahmen seien in der Regel die Kommunen zuständig. Der SPD-Datenschutzexperte Florian Ritter sieht dagegen die Staatsregierung in der Pflicht und forderte Aufklärung: Die Anlagen müssten sofort abgeschaltet werden, bis die gesetzlichen Regeln sicher eingehalten werden: „Da an den Schulen weder das juristische noch technische Know-how vorhanden sein kann, ist die Staatsregierung verantwortlich, dass – wenn die Videoüberwachung schon eingesetzt werden muss – dies auch nach Recht und Gesetz geschieht.“ Auch die Grünen reagierten empört durch die Landtagsabgeordnete Verena Osgyan: „Wenn auf Videoüberwachung nicht klar hingewiesen wird, dann ist das ein eklatanter Verstoß gegen den Datenschutz.“

Minderjährige Schüler seien besonders schutzwürdig und dürften per Überwachung nicht unter Generalverdacht gestellt werden.

In Bad Abbach (Lkr. Kelheim) gibt es z. B. fünf Kameras an der Mittelschule und vier Kameras an der Grundschule. In Schwandorf gibt es an der Berufsschule und am Gymnasium jeweils sechs Kameras. Am Gymnasium in Nabburg (Lkr. Schwandorf) sind vier Kameras installiert. An der Grundschule Bodenwöhr (Lkr. Schwandorf) gibt es fünf Kameras. An der Telemann-Grund- und Mittelschule in Teublitz (Lkr. Schwandorf) sind sieben Kameras installiert (Stand 2012). Nach dem Amoklauf von Winnenden im Jahr 2009, bei dem ein 17-Jähriger an einer Realschule neun SchülerInnen und drei Lehrerinnen erschoss, hatten viele Schulen auch Videokameras installiert in der falschen Hoffnung, damit solche Taten verhindern zu können (Heimliche Bilder, verbotene Töne, SZ 01.12.2014, 40; Hawranek/Zierer, Kameras an Schulen empören Datenschützer, www.br.de 01.12.2014).

Hessen

Klinikpersonal las unerlaubt Tugces Patientenakte

Als die Studentin Tugce Albayrak um ihr Leben rang, haben rund 90 Krankenhaus-Mitarbeitende illegal ihre Akte gelesen. Die Frau starb an ihrem 23. Geburtstag am 02.12.14. Nur direkt mit der Behandlung des jeweiligen Patienten betraute Ärzte und Pfleger dürfen die Krankenakten einsehen. Der Geschäftsführer des Sana-Klinikums Sascha John bestätigte die unzulässigen Datenzugriffe. Das Schicksal der Studentin habe alle Menschen, auch die Klinikmitarbeitenden, „emotional sehr angegriffen. Das war die Hauptmotivation." Menschlich sei das nachvollziehbar, zu entschuldigen sei es aber nicht. Derzeit werde mit allen Beschuldigten gesprochen. Ihnen drohen Ab- oder Ermahnungen, Kündigungen wurden bisher nicht ausgesprochen. Man habe keine Hinweise darauf, dass jemand Unterlagen kopiert und weitergegeben habe.

Ans Licht gekommen war der Fall, weil das Datensystem der Klinik für November 2014 überdurchschnittlich viele Zugriffe auf Krankenakten auswies. Als die Klinikleitung nach dem Grund suchte, fiel die Häufung bei der Patientin auf. Die Studentin aus Gelnhausen war Mitte November 2014 vor einem Fast-Food-Lokal in Offenbach niedergeschlagen und lebensgefährlich verletzt worden. Knapp zwei Wochen lang lag sie im Koma, bevor die lebenserhaltenden Maschinen abgeschaltet wurden. Sie soll vor der Prügelattacke zwei minderjährigen Schülerinnen zu Hilfe gekommen sein, die in der Toilette von dem Beschuldigten und seiner Clique bedrängt worden sein. An ihrem Schicksal hatten Millionen Anteil genommen, insbesondere in den sozialen Netzwerken. Der Hauptverdächtige, ein 18-Jähriger, sitzt in Haft (Klinikpersonal las unerlaubt Tugces Akte, www.n-tv.de 30.01.2015).

Niedersachsen

Barbara Thiel wird neue Datenschutzbeauftragte

Auf Vorschlag der Landesregierung wählte der Niedersächsische Landtag am 18.12.2014 in Hannover Barbara Thiel einstimmig zur Landesbeauftragten für den Datenschutz (LfD) Niedersachsen. Da es für die Wahl der LfD einer 2/3-Mehrheit im Landtag bedarf, musste die Landesregierung sich mit der CDU auf eine gemeinsame Kandidatin einigen. Zuvor hatte die Landesregierung den Vorschlag der CDU-Fraktion abgelehnt, Gert Hahne, Referatsleiter und ehemaliger Sprecher im Agrarministerium, zum LfD zu machen. Auch über andere Vorschläge konnte zunächst keine Einigung hergestellt werden. Die 59-jährige Juristin Thiel übernahm das Amt am 01.01.2015 und ist damit Nachfolgerin von Joachim Wahlbrink, der das Amt seit 2006 bekleidet und dessen Amtszeit offiziell am 01.06.2014 auslief. Sie ist die erste Frau in diesem Amt. Barbara Thiel wurde nach der Wahl von der Landesregierung auf die Dauer von acht Jahren berufen.

Die CDU-Politikerin sagte nach ihrer Ernennung, sie wolle nicht nur still im Hintergrund tätig werden, sondern auch öffentlich dem Datenschutz eine Stimme geben. Die von allen Seiten angebotene gute Zusammenarbeit wertete die 59-Jährige als gute Basis: „Ich habe großen Respekt vor diesem Amt, weil ich der Auffassung bin, dass Datenschutz in Zeiten der Digitalisierung immer mehr an Bedeutung gewinnt." Sie sehe ihre Stelle als Begleiter und Wächter der Landesregierung zugleich. Innenminister Boris Pistorius (SPD) nannte sie bei der Übergabe der Ernennungsurkunde eine gute Wahl, bei der der Datenschutz in guten Händen sei. Ihren wegen Krankheit abwesenden Vorgänger würdigte er wegen dessen „engagierter und leiser Aufgabenwahrnehmung": „Er hat sich nicht zum Ankläger bei Datenschutzverstößen aufgeschwungen, sondern er hat den Mahner gemacht, er hat den Berater gemacht, er hat den Blick geöffnet für Datenschutzfragen des 21. Jahrhunderts."

Barbara Thiel wuchs in Salzgitter auf. Nach ihrem beruflichen Einstieg bei der Stadt Salzgitter, dem Jurastudium in Göttingen und der Referendarzeit in Niedersachsen war sie in der Bezirksregierung Braunschweig, im Niedersächsischen Innenministerium, beim Niedersächsischen Landesrechnungshof sowie beim Landkreis Wolfenbüttel tätig. Vor ihrer Übernahme des Amtes der LfD leitete sie das Dezernat Öffentliche Gesundheit, Sicherheit, IT-Koordination und EU-Angelegenheiten bei der Region Hannover.

Thiel wird Chefin von 30 Mitarbeiterinnen und Mitarbeitern. Jährlich bearbeiten sie mehr als 3.000 Eingaben. Im der Behörde angegliederten Datenschutzinstitut Niedersachsen gibt es ein Schulungsangebot mit Kursen, Seminaren, Workshops und Gesprächskreisen. Unter www.lfd.niedersachsen.de bietet die Behörde zudem eine Fülle an Informationen zu verschiedensten Datenschutzthemen an (Landtag wählt Barbara Thiel zur Nachfolgerin von Joachim Wahlbrink, www.datenschutz.de 21.12.2014; Erstmals Frau zur Datenschutz-Hüterin gewählt, www.welt.de 19.12.2014).

Rheinland-Pfalz

Debeka zahlt Millionen-Geldbuße

Die im Dezember 2013 eingeleiteten Ordnungswidrigkeitenverfahren des

rheinland-pfälzische Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI), Edgar Wagner, gegen den Debeka-Krankenversicherungsverein a. G. (Debeka) und seine Vorstandsmitglieder wurden mit einer Verständigung über eine Geldbuße in Höhe von 1,3 Millionen Euro am 29.12.2014 abgeschlossen. Vorstand und Aufsichtsrat des Unternehmens haben die Geldbuße bereits akzeptiert. Weitere 600.000 Euro stellt die Debeka für eine Stiftungsprofessur zum Thema Datenschutz an der Johannes Gutenberg-Universität Mainz bereit. Damit soll die Debeka die Grundlagenforschung für einen effektiven Datenschutz und dessen Implementierung in der Praxis fördern.

Der LfDI überprüfte umfassend die Zusammenarbeit der Debeka mit Tippgebern. Der Vorwurf bestand darin, dass über die Tippgeber im öffentlichen Dienst illegal Adressdaten von BeamtenanwärterInnen angekauft wurden, so dass sich der private Krankenversicherer Wettbewerbsvorteile verschafft hatte. Das Datenschutzrecht steht nach Auffassung des LfDI dem Einsatz von Tippgebern nicht grundsätzlich entgegen. Unter beratender Einbeziehung des LfDI wurde der Vertrieb mit Tippgebern bei der Debeka so ausgerichtet, dass die Arbeit der Tippgeber nach Ansicht des LfDI sogar über die gesetzlichen Standards für den Datenschutz hinausgeht. Eine Weitergabe von Adressen über Tippgeber soll zukünftig nur noch bei Vorliegen einer förmlichen Einwilligungserklärung jedes einzelnen Betroffenen erfolgen.

Die Debeka und der LfDI sprechen übereinstimmend von einer konstruktiven Aufarbeitung der datenschutzrelevanten Vorgänge im Vertrieb der Debeka. Die Verfahren gegen die Vorstände sind ohne Bußgeldzahlungen eingestellt worden. Anlass der Untersuchungen waren vom Unternehmen eingeräumte Fälle sogenannter Listenkäufe, bei denen einzelne Mitarbeitende weisungswidrig Datensätze zu Anwärtern im öffentlichen Dienst erworben und genutzt hatten. Der LfDI stellte fest, dass datenschutzwidrig Neukunden für die Debeka durch Informationen von Kollegen gewonnen wurden. Einzelne Debeka-Mitarbeitende hatten Listen oder Kontaktdaten möglicher KundInnen ohne deren Einverständnis erhalten und dafür ein Entgelt bezahlt. Hierbei verstießen sie gegen unternehmensinterne Vorgaben, aber auch gegen geltendes Datenschutzrecht. Die Debeka musste feststellen, dass in der Vergangenheit nicht alle Aufsichtsmaßnahmen und Kontrollen etabliert und angewandt worden waren, die aus heutiger datenschutzrechtlicher Sicht den notwendigen Standards entsprechen. Seit 2013 sind solche Aufsichtspflichtverletzungen mit erheblich gesteigerten Bußgeldern bedroht, die nun erstmals auch verhängt wurden.

Bei der Höhe der Bußgeldbemessung wurden zugunsten der Debeka ihre umfassende Kooperation mit dem LfDI, ihre eigene Aufklärung sowie die zugesagte Stiftungsprofessur berücksichtigt. Auch die Bereitschaft der Debeka, bei der Anwerbung neuer KundInnen künftig strikt auf die Einhaltung einschlägiger Datenschutzvorschriften zu achten, wurden einbezogen sowie die vorbildliche Optimierung einer neuen, weitgreifenden internen Datenschutzstruktur. Berücksichtigt wurde ferner, dass in der Vergangenheit auch seitens der öffentlichen Dienstherren keine hinreichenden Maßnahmen zur Wahrung des Datenschutzes getroffen worden waren.

Die Vorwürfe führten 2013 nicht nur zum Tätigwerden des LfDI. Die Finanzaufsicht Bafin hat ihre Prüfung im Mai 2014 abgeschlossen. Sie hat die Debeka wegen Mängeln in Organisation und Kontrolle gerügt, aber keine Sanktionen verhängt. Die Bafin veröffentlichte Ende 2014 Regeln für die Zusammenarbeit mit Tippgebern im öffentlichen Dienst, die auch bei anderen Versicherern üblich ist. Die Staatsanwaltschaft Koblenz ermittelt seit Juli 2014 gegen einzelne Debeka-Mitarbeitende und Angehörige des öffentlichen Dienstes; die Untersuchungen sind nicht abgeschlossen.

Edgar Wagner erklärte: „Wichtiger als das verhängte Bußgeld ist mir zweierlei: Zum einen hat die Debeka ernsthafte und erfolgreiche Anstrengungen unternommen, den Datenschutz in ihrem Vertriebssystem zu stärken. Ohne das kooperative Verhalten der Debeka wäre ein solch gutes Ergebnis nicht zu erzielen gewesen. Zum anderen geht von dem Verfahren das Signal aus, dass alle Unternehmen zukünftig mit noch mehr Nachdruck daran arbeiten müssen – und können! -, dass mit den persönlichen Daten von Interessenten, Kunden und Mitarbeitern vertrauensvoll und rechtskonform umgegangen wird.“ Auch im öffentlichen Bereich seien durch die Änderung der Nebentätigkeitsbestimmungen und durch die Aufarbeitung von Datenschutzverstößen erste wichtige Konsequenzen gezogen und die Überwachungs- und Kontrollmechanismen den heute geltenden Standards angepasst worden (PE LfDI Rheinland-Pfalz v. 29.12.2013, Bußgeldverfahren gegen die Debeka einvernehmlich abgeschlossen; Debeka zahlt Millionen-Geldbuße, SZ 30.12.2014, 25).

Thüringen

Umbau des Verfassungsschutzes

In der Koalitionsvereinbarung des neuen rot-rot-grünen Regierungsbündnisses in Thüringen haben die Linken, die SPD und Bündnis 90/Die Grünen vereinbart, den dortigen Landesverfassungsschutz zu entmachten und das System der V-Leute, die nur unter sehr strengen Voraussetzungen zugelassen werden sollen, zurückzufahren. In Thüringen gibt es viele Beispiele, nicht nur im Zusammenhang mit den NSU-TerroristInnen, bei denen der Verfassungsschutz am Aufbau extremistischer Strukturen aktiv mitgewirkt hat. Thüringen wird so zum Testfall, ob bei der Wahrnehmung der Verfassungsschutzaufgaben auf V-Leute weitgehend verzichtet werden kann (Schultz, SZ 22./23.11.2014, 4).

Datenschutznachrichten aus dem Ausland

Frankreich

Gelber Obdachlosen-Ausweis in Marseille

Marseilles Vize-Bürgermeister Xavier Méry und der Direktor von Samu Marseille René Giancarli wollen Obdachlosen in Marseille einen „Gesundheitsausweis“ geben. Im Notfall sollen Rettungskräfte dort lebensrettende Informationen finden. Das Dokument enthält auf der Vorderseite ein auffälliges gelbes Dreieck und erinnert so an den Judenstern, der zur öffentlichen Kennzeichnung im deutschen Nationalsozialismus verwendet wurde. „Samu Social“ ist eine Hilfsorganisation, deren freiwillige Retter und Sozialaktivisten sich seit Jahr und Tag um arme Menschen in der Metropole am Mittelmeer kümmern, auch um die SDF („sans domicile fixe“), wie die Franzosen ihre Obdachlosen nennen.

Giancarli hatte die Idee mit dem „Gesundheitsausweis“. Jeder Obdachlose solle eine etwa handgroße Karte bekommen und möglichst gut sichtbar tragen – am Anorak, am Rucksack oder irgendwo an der Hose. Auf dem Karton werde alles vermerkt, was Helfende notfalls wissen sollten: Name und Vorname des Clochards, seine Sozialversicherungsnummer, seine Allergien und chronischen Krankheiten. Damit die Karte auch schnell erkannt wird, prangt darauf ein großes, leuchtend gelbes Dreieck mit einem dicken Ausrufezeichen in der Mitte, das sich bei genauem Hinsehen als ein Thermometer entpuppt. Die Farbe Gelb und das Thermometer, so Giancarli, seien schließlich „überall auf der Welt“ die Symbole der Lebensretter.

Samu und die Stadt ließen 1500 Exemplare drucken. 300 waren verteilt, als ein Sturm der Entrüstung losbrach. Sozialpolitiker warnten, der Ausweis mit dem gelben Dreieck „diskriminiert und stigmatisiert eine Minderheit“. Ärzte nannten Marseilles SDF-Pass „einen Gipfel der Dummheit“, und die Liga für Menschenrechte warnte, das Emblem „erinnert zwangsläufig an den gelben Stern, den Juden tragen mussten“ während der Besetzung Frankreichs durch deutsche Nazi-Truppen. Anfang Dezember 2014 zogen 150 Demonstranten vors Rathaus von Marseille; auf Plakaten führten sie der Stadtverwaltung die Ähnlichkeit von Judenstern und SDF-Dreieck bildhaft vor Augen. Marisol Touraine, die sozialistische Gesundheitsministerin Frankreichs, geißelte den Ausweis als „inakzeptabel“ und verlangte, die Maßnahme unverzüglich einzustellen.

Die Verantwortlichen gaben sich betroffen. Méry, der der konservativen Oppositionspartei UMP angehört, gab sich „schockiert und zutiefst empört über diese absurde Polemik“ ob des Vergleichs „mit den düstersten Kapiteln unserer Geschichte“. Und Samu-Chef Giancarli beteuerte, an den Judenstern habe er „niemals gedacht“. Er habe seinen Clochards „doch nur einen Namen, nur eine Identität“ geben wollen. Giancarli erzählte, wie er vor Jahren einmal einen toten SDF auf der Straße gefunden habe, und dass damals Monate vergangen seien, ehe man den Leichnam habe identifizieren und begraben können. Marseilles Ober-Samu ist sicher, dass – sobald der Wirbel abgeklungen sei – sich seine „gute Idee“ noch durchsetzen wird: „Sie werden sehen, bald wollen alle die Karte haben.“

Nach der öffentlichen Kritik wollen Stadt und Samu Social nachbessern. Auch Sozialarbeiter und freiwillige Helfer aus den Reihen der Samu Social hatten Datenschutz-Bedenken angemeldet. Ein neuer Ausweis wird gedruckt, ohne Hinweis aus der Krankenakte. Für die Stadt hat Xavier Méry klargestellt, die Karte sei „eben eine Karte, also kein Badge, den man sichtbar tragen muss“. Das gelbe Dreieck soll aber bleiben (Wernicke, Mistral der Empörung, SZ 06./07.12.2014, 10).

Frankreich

AXA erfasst Fitness- und Fahrdaten

Der Versicherungskonzern AXA kooperiert künftig mit dem Elektronikhersteller Samsung. Vorerst gibt es das Angebot nur für Frankreich, doch wenn es der Wettbewerb will, bald auch in Deutschland: AXA will die Samsung-Armbanduhr Gear 3 für die Erfassung von Fitnessdaten nutzen und für Erinnerungen per App. Die Gear 3 funktioniert nur zusammen mit einem Samsung-Handy. AXA geht es nach eigenem Bekunden ausschließlich darum, dass die KundInnen fitter werden, so eine Sprecherin: „Wir wollen die Gesundheit und das Wohlbefinden unserer Kunden steigern. Die AXA-Health-App will erreichen, dass die Kunden sich 24 Stunden am Tag und sieben Tage die Woche beschützt fühlen. Sie können dadurch für sich und ihre Familien einen gesünderen Lebensstil erreichen.“ In Deutschland plant der Konzern bislang kein ähnliches Angebot, doch meint ein Sprecher in Köln: „Wir bieten ein Bonusprogramm bei Erreichen bestimmter Gesundheitsziele an, zum Beispiel einen bestimmten Body-Mass-Index.“ Das funktioniert bislang per Formular und ärztliche Bestätigung.

Die Konkurrenz der Versicherer um digitale Informationen ist heftig. Wer als Erster die Kundendaten geschickt auswertet, hofft auf einen Wettbewerbsvorteil. Vier Wochen zuvor hatte der AXA-Rivale Generali eine Vereinbarung mit dem südafrikanischen Dienstleister Discovery geschlossen. Die KundInnen erhalten Gutscheine und Rabatte, wenn sie ihr Bewegungs- und Ernährungsverhalten dokumentieren (in diesem Heft S. 32). AXA investiert kräftig: 800 Millionen Euro hat Konzernchef Henri de Castries für die Jahre 2013 bis 2015 bereitgestellt. Ein eigenes Labor im Silicon Valley hilft bei der Entwicklung. Der Datenschutz ist nach Auskunft von Veronique Weill aus dem Pariser AXA-Vorstand gesichert: „Wir suchen immer die Zustimmung des Kunden. Wenn er uns seine Daten gibt, können wir sein Risiko besser einschätzen und ihm einen besseren Preis geben.“

Ein anderes Projekt zeigt, in welche Richtung AXA denkt: Die Versicherung will herausfinden, wie sie aus Route und

Fahrstil darauf schließen kann, wer am Steuer sitzt. Sie möchte einen individuellen Fingerabdruck für jeden Fahrenden ermitteln. Findet AXA eine Lösung, kann sie sichere von unsicheren Fahrenden trennen, um ihnen höhere Preise berechnen zu können und um in der Konkurrenz um die guten Fahrenden die Nase vorn zu haben. Außerdem könnte der Versicherer kontrollieren, ob wirklich nur die ihm gemeldeten Fahrenden am Steuer sitzen. Am 15.12.2014 hat das Unternehmen deshalb ein Preisgeld von 15.000 Dollar ausgesetzt. Bislang haben sich 64 Forscherteams für den Wettbewerb angemeldet. Aus der Ausschreibung geht hervor, welche Informationen AXA interessieren: „Fährt ein Fahrer lange Strecken oder kurze? Fährt er auf Autobahnen oder Nebenstraßen? Beschleunigt er kräftig aus dem Stand? Fährt er mit hoher Geschwindigkeit durch Kurven?“

Die deutsche AXA hält sich bislang auch in der Digitalisierung der Autoversicherung zurück. Doch ermöglicht ihre „AXA Drive App“ es KundInnen und anderen Interessierten schon heute, das eigene Fahrverhalten zu analysieren. Gemessen werden Beschleunigungs- und Bremsverhalten sowie das Fahren in Kurven. Noch werden die Daten nicht zum Versicherer übertragen. Die AXA testet das Programm und setzt auf den Spieltrieb der Nutzer. Auf der AXA-Website heißt es: „Durch richtiges Verhalten können Sie Punkte sammeln und in immer höhere Leistungsstufen aufsteigen. Und damit das alles noch mehr Spaß macht, können Sie über soziale Netzwerke Ihren Status und Ihre Punkte mit anderen teilen“ (Fromme, Wer läuft, zahlt weniger, SZ 18.12.2014, 24).

Großbritannien

Steinmetz mit Datenschutz gegen Korruptionsbericht

Die britische Nichtregierungsorganisation Global Witness kritisierte in einem Report 2013 die Firmen BSGR und Onyx Financial Advisors des 58jährigen milliardenschweren Rohstoffhändlers Beny Steinmetz, den insbesondere Diamanten reich gemacht haben. Gemäß den Recherchen von Global Witness haben Mitarbeitende von BSGR Politiker bestochen. Dem Präsidenten des westafrikanischen Staats Guinea und seiner Frau sollen Millionen Dollar Schmiergeld versprochen worden sein, um Zugang zu dem bergigen Simandou-Gelände zu sichern, wo enorme Eisenerz-Reserven vermutet werden. Die Firmen widersprechen den Vorwürfen.

Steinmetz versuchte gemeinsam mit drei weiteren Mitarbeitern, gegen den Korruptionsbericht von Global Witness vorzugehen; sie riefen über Anwälte den Datenschutzbeauftragten des Vereinigten Königreichs an. Der Aktivistenreport verstoße gegen ihre Datenschutzrechte. Gemäß dem britischen Recht können Personen Auskunft verlangen, welche Daten Organisationen über sie gespeichert haben. Global Witness berief sich auf die Pressefreiheit, die beeinträchtigt würde, wenn sie offenbaren müssten, was sie von wem wüssten. Ihre Quellen seien in Gefahr. Der Datenschutzbeauftragte folgte der Argumentation und wies den Antrag von Steinmetz ab: Für Global Witness gelte wie für Medien eine Ausnahme, da sie die Öffentlichkeit aufklären wollen. Steinmetz will gegen die Entscheidung gerichtlich vorgehen (Korrumpierte Privatsphäre, SZ 23.12.2014, 18).

USA

FBI überwacht Mobilkommunikation ohne Gerichtsbeschluss

Die US-amerikanische Ermittlungsbehörde FBI meint, für Einsätze von Funkmastensimulatoren (IMSI-Catcher) an öffentlichen Orten keinen Gerichtsbeschluss zu benötigen. Das geht aus einem Schreiben zweier US-Senatoren an den US-Justizminister Eric Holder hervor. Darin zeigen sich der Vorsitzende des Justizausschusses des Senats, der Demokrat Patrick Leahy, und der Republikaner Chuck Grassley besorgt über den Schutz der Privatsphäre unbescholtener US-BürgerInnen. Normalerweise benötigt das FBI für den Einsatz von IMSI-Catchern zur Handyüberwachung einen richterlichen Beschuss.

Hintergrund des Anschreibens sind Enthüllungen vom November 2014 über die Überwachung von Handys aus Flugzeugen heraus. Der United States Marshals Service habe dafür speziell ausgerüstete Kleinflugzeuge vom Typ Cesna, hieß es, in denen Geräte angebracht sind, die als falsche Handymasten alle Mobiltelefone in der Nähe dazu bringen, sich mit ihnen zu verbinden. Ist das Gerät einer gesuchten Person darunter, werde das herausgefiltert und dank der Positionsänderung des Flugzeugs könne es dann bis auf drei Meter genau lokalisiert werden. Dass gleichzeitig unzählige Unschuldige ins Visier der Behörde geraten, werde dabei in Kauf genommen. Hieran stören sich Leahy und Grassley. Sie hatten bereits im Juni 2014 FBI-Direktor James Comey um Informationen zur Überwachung mit Funkzellensimulatoren gebeten. Zwar gebe es Bestimmungen, laut denen die Ermittler eine richterliche Genehmigung benötigen, aber auch einige Ausnahmen davon. Diese erscheinen Leahy und Grassley weit gefasst. Diese Ausnahmen gelten in Fällen, in denen die öffentliche Sicherheit massiv gefährdet ist, in denen ein Flüchtender beteiligt ist oder in denen die Technik an Orten angewendet wird, „in denen nicht mit Privatsphäre zu rechnen“ sei. Die beiden Senatoren wollen geklärt haben, unter welchen Umständen das FBI die Überwachungstechnik anwendet und wie sie von anderen Behörden gehandhabt wird, zum Beispiel dem Department of Homeland Security. Das FBI ist dem US-Justizministerium untergeordnet.

Auch im Juni 2014 hatten die Bürgerrechtsorganisation American Civil Liberties Union mehr über die Überwachung per IMSI-Catcher wissen wollen und Akteneinsicht nach Informationsfreiheitsgesetzen mehrerer Staaten beantragt. Die Polizei der Stadt Sarasota in Florida bot die daraufhin einen Termin zur Akteneinsicht an. Doch dann beschlagnahmten Bundesbeamte die Akten. So werde die Stadtpolizei daran gehindert, die gesetzlich vorgesehene Auskunft zu erteilen (FBI überwacht Handys mit IMSI-Catchern auch ohne Gerichtsbeschluss, www.heise.de 07.01.2015).

USA

Empörung über europäische „Daten-Lokalisierung“

Vergaberegelungen in Deutschland und Frankreich erzürnen die US-Wirtschaft, weil von ihnen diskriminierende Handelshindernisse ausgingen. Bei der Vergabe von staatlichen Aufträgen, so die öffentliche Äußerung des US-Handelsvertreters bei der Computer and Communications Industry Association (CCIA), werde gefordert, dass das beauftragte Unternehmen die Datenspeicherung und -verarbeitung innerhalb des Landes gewährleisten müsse. Die französische Regierung habe noch keine neuen Gesetze vorgeschlagen und warte auf eine EU-Richtlinie zur Cybersicherheit, die innerhalb der nächsten sechs Monate kommen werde. Demgegenüber würden von der deutschen Regierung neue Regeln schon umgesetzt. Die Regierungen beider Länder würden verlangen, dass die Daten der eigenen Bürgerinnen und Bürger von den Unternehmen vor Ort verarbeitet werden müssten. In ihrer Veröffentlichung vom 29.10.2014 behauptet die CCIA: „Anforderungen an die Lokalität von Datenverarbeitung stehen im Widerspruch zu weltweiten Handelsnormen, wonach handelsbeschränkende Maßnahmen nur erlaubt sind, wenn diese zur Erreichung eines legitimen nationalen Sicherheitsinteresses oder eines Gemeinwohlziels erforderlich sind und weniger restriktive Maßnahmen zur Zielerreichung nicht bestehen.“ Außerdem seien die Regelungen oft äußerst unbestimmt formuliert.

Chris Wolf, Leiter der globalen Privacy-Abteilung der Rechtsfirma Hogan Lovells, behauptete, die erzwungene Lokalisierung von Datenverarbeitung stehe im Widerspruch zu Safe Harbor, dessen Ziel es sei, unter bestimmten Umständen einen unbeschränkten Datenfluss zwischen der EU und den USA zu ermöglichen. Es gäbe für die Unternehmen keine Möglichkeit der Gegenwehr, wenn ihnen von einem EU-Mitgliedstaat Datentransfers in die USA verboten würden, außer die US-Regierung um Unterstützung zu bitten. Deshalb müsse über den „Aberwitz der Datenlokalisierung“ aufgeklärt werden. Im Europäischen Parlament gäbe es Stimmen, Safe Harbor aufzuheben. Gespräche über eine Aktualisierung von Safe Harbor kommen nicht voran, nachdem die USA sich nicht bereit erklärt hat, gemäß der Forderung der EU-Kommission den Umfang der Ausnahmen im Interesse der nationalen Sicherheit einzuschränken. Diese Ausnahmen beziehen sich auf Datenabfragen für Zwecke der Strafverfolgung und durch Geheimdienste. Wegen der erzwungenen Lokalisierung und der Ungewissheit der Zukunft von Safe Harbor forderte Wolf, das Thema des grenzüberschreitenden Datenflusses bei den Freihandelsverhandlungen zwischen den USA und der EU zu thematisieren. Der Vertreter des Handelsministeriums Ted Dean, der für die USA die Safe Harbor-Reform verhandelt, wollte sich nicht darauf festlegen, wann die USA auf die EU-Forderung reagieren werde. US-Wirtschaftsvertreter meinten, mit den Restriktionen bei der Datenverarbeitung würden die beabsichtigten Ziele – die Stärkung der heimischen Wirtschaft und der Schutz von Ausspähung durch Regierungsstellen – nicht erreicht. Wolf meinte, dass vielmehr ein Wirtschaftswachstum behindert werde, weil dadurch Cloud Computing ineffektiv werde. Außerdem seien lokal gespeicherte Daten leichter angreifbar als Daten, die auf verschiedenen Rechnern gespeichert werden (U.S. Businesses Object To French, German Proposals To Restrict Data, Inside U.S. Trade – 11/21/2014, www.ccianet.org).

USA

DEA nutzt ein Facebook-Fakeprofil mit Echtdaten

Sondra Arquiett, eine braunhaarige 28jährige Mutter eines Sohnes in New York/USA, verklagte einen Agenten der US-amerikanischen Drogenbehörde Drug Enforcement Administration (DEA) wegen der Verletzung ihrer Persönlichkeitsrechte. Sie wirft Timothy Sinnigen vor, einen gefälschten Facebook-Account unter ihrem Namen angelegt und vier Jahre betrieben zu haben. Hierfür hat der DEA-Mitarbeiter Arquietts Informationen und Bilder von deren Mobiltelefon gestohlen und sie als Lockvogel genutzt. Auf dem Facebook-Profil rekelte sich die junge Frau in Hotpants auf der Motorhaube eines silbernen BMWs oder hielt ihren Sohn und eine Nichte im Arm. Arquiett fordert eine Entschädigung von 250.000 Dollar (ca. 200.000 Euro). Sie war im Jahr 2010 mit einem Drogendealer liiert und wegen des Besitzes von Kokain verhaftet worden; sie kooperierte mit der Polizei, stellte ihr Mobiltelefon zur Verfügung und wurde zu einer Bewährungsstrafe verurteilt. Während sie auf ihr Urteil wartete, soll die DEA das Fake-Profil von ihr ins Netz gestellt haben, um mit anderen Verdächtigen des Drogenrings in Kontakt zu kommen.

Gemäß Gerichtsunterlagen soll das Justizministerium das Vorgehen im August 2014 wie folgt gerechtfertigt haben: Mit der Erlaubnis zur Durchsuchung des Mobiltelefons sei implizit auch die Erlaubnis zur Datennutzung für Ermittlungszwecke erteilt worden. Das Justizministerium hatte zuerst das Vorgehen des Drogenfahnders verteidigt. Ein Tag nach dem ersten Bericht über den Vorgang ließ es jedoch verlautbaren, man wolle diese Ermittlungspraxis überprüfen. Seit dem 07.10.2014 ist der Fake-Account bei Facebook nicht mehr zu erreichen. Facebook hat offensichtlich dafür gemäß seinen Nutzungsnutzrichtlinien, die Fake-Accounts nicht zulassen, gesorgt (Grasshoff, Fakebook statt Facebook, SZ 09.10.2014, 9).

USA

Uber analysiert Nutzungsdaten

Nutzende der Taxi-Konkurrenz-App Uber verraten offenbar durch ihr Fahrverhalten mehr als ihnen lieb ist: Der Dienst hat anhand der nächtlichen Bestellungen ausgewertet, welche KundInnen wohl zu einem One-Night-Stand unterwegs waren und die Ergebnisse dieser Analyse in einem Blog-Eintrag veröffentlicht.

Der Beitrag stammt aus dem Jahr 2012 und ist mittlerweile gelöscht. JournalistInnen haben sich jetzt genauer mit dieser Praxis befasst und die Firma konfrontiert. Bereits im November 2014

hatte unter anderem ein amerikanische Lokalsender in San Francisco den entsprechenden Blogeintrag gefunden und das Verfahren erklärt. Demnach wurden Fahrgäste statistisch erfasst, die freitags oder samstags zwischen 22 Uhr abends und 4 Uhr morgens einen Uber-Wagen buchten – und vier bis sechs Stunden später eine weitere Fahrt von einem Punkt innerhalb von 160 Metern des Ortes aus, an dem sie zuvor abgesetzt wurden, bestellten. „Rides of Glory“ nannte Uber solche Fahrten im entsprechenden Blogeintrag. Später wurden laut Firmenangaben auch andere Wochentage ausgewertet – und es habe sich gezeigt, dass sich solche Fahrten insbesondere um bestimmte Feiertage herum häufen. Gemäß Medienberichten hat Uber auf Grundlage der ermittelten Daten Karten von New York, San Francisco und anderen US-Städten erstellt, in denen die Bezirke mit besonders vielen möglichen One-Night-Stands rot markiert wurden.

Uber-Deutschlandchef Fabien Nestmann verteidigte die Analyse. Er bezeichnete eine Auswertung von Nutzungsdaten hinsichtlich solcher Kurzaufenthalte als „analytisches Spiel“ und verteidigte die umfangreiche Sammlung der Daten: „Man kann aus sämtlichen Auswertungen Rückschlüsse ziehen, die helfen können, das Angebot zu verbessern. Das ist Teil der Aktivität, die Uber machen muss und wird.“ Gelöscht werden die Nutzungsdaten Nestmann zufolge nur, wenn eine NutzerIn die Firma explizit dazu auffordert. Die Sammlung von Nutzungsdaten ist dem Deutschlandchef zufolge „Teil des Konzepts“ des Fahrtenvermittlers, in den Google mehr als eine Viertelmilliarde Dollar investiert hat. Künftig werde man sich allerdings darauf konzentrieren, „sinnvolle Auswertungen zu machen“ (Uber analysiert One-Night-Stands seiner Nutzer, www.spiegel.de 08.01.2015).

Afghanistan

Deutsche Datenlieferung – Tötung durch US- und britisches Militär

Das Bundesverteidigungsministerium bestätigte Berichte, wonach die Bundeswehr bei der Erstellung von Listen mit afghanischen Aufständischen mitwirkten, die von US-amerikanischem und britischem Militär zu deren Tötung genutzt wurden. Es habe aber nie eine Empfehlung zur Tötung gegeben, sondern lediglich zur „Festsetzung“ dieser Personen. Allerdings hat die US-Armee viele der aufgelisteten Taliban-Führer getötet.

- Deutsche Zieldaten

Im deutschen Hauptquartier in Masar-i-Scharif in Afghanistan gab es eine sogenannte Target Support Cell, deren Auftrag es war, „Informationen für die Nominierung möglicher Personenziele zu sammeln“. Die Soldaten erstellten „Ziel-Ordner“, die zur Genehmigung vorgelegt wurden. Bei einer Besprechung im Mai 2011 hatte z. B. ein hochrangiger Soldat gefordert, es als „Priorität“ zu behandeln, einen Aufständischen namens Kari Hafis ausfindig zu machen. Dieser solle festgenommen oder „neutralisiert“ werden. Bei anderen Aufständischen hatten gemäß Presseberichten Beteiligte an den Sitzungen zu bedenken gegeben, dass ihre Beseitigung ein gefährliches Machtvakuum hinterlassen würde, da sie über viel Macht, Waffen, Geld und Drogen verfügten.

Gemäß Presseberichten genehmigte der Bundesnachrichtendienst (BND), dass von ihm gesammelte Informationen im Fall eines drohenden Angriffs zur gezielten Tötung von „Personenzielen“ eingesetzt werden können. Die Berichte zitieren aus einem geheimen BND-Dokument von August 2011 zum Taliban-Führer Kari Jusuf. Demnach übermittelte der BND auch Telefonnummern, die zur Ortung von Jusuf eingesetzt werden konnten.

Der frühere Nato-General Egon Ramms bestätigte, dass Deutschland Zieldaten für die Tötung von Taliban-Kämpfern in Afghanistan geliefert hat. Deutschland habe an der Zielerfassung mitgearbeitet, nachdem die Bundesregierung im Februar 2010 die Situation als Krieg eingestuft habe. Es habe Tötungslisten gegeben, die nicht nur von den USA und Großbritannien alleine erarbeitet worden seien: „Sie können sie auch als Nato-Listen bezeichnen, weil sie also auf den verschiedenen Ebenen der Regionalkommandos in Afghanistan und auch im Isaf-Hauptquartier entsprechend erarbeitet worden sind.“ Die Bundeswehr führt das Regionalkommando Nord der internationalen Schutztruppe Isaf seit 2006. Ramms war bis September 2010 Befehlshaber der Nato-Kommandozentrale im niederländischen Brunssum, die den Afghanistan-Einsatz leitete.

Die Praxis gezielter Tötungen von Aufständischen ist international hoch umstritten. Besonders die US-Streitkräfte fliegen in Afghanistan und Pakistan seit Jahren regelmäßig Angriffe auf mutmaßliche Rebellenführer und andere Extremisten. In Deutschland wird seit langem darüber diskutiert, welchen Anteil der BND und die Bundeswehr an den umstrittenen Drohnenangriffen haben. Dabei geht es insbesondere um die Weitergabe von Telefonnummern von Verdächtigen, die von Geheimdiensten zu ihrer Ortung benutzt werden können.

Die Presse berichtete von einer Liste, auf der zeitweise 750 Personen standen, auf der die USA und ihre Nato-Verbündeten Personenziele für das „targeted killing“ führten. Erfasst sind darin nicht nur der Führungskreis der Taliban, sondern auch die mittlere und die untere Ebene. Einige Afghanen seien nur auf der Liste geführt worden, weil sie die Aufständischen angeblich als Drogenhändler unterstützten. Im Oktober 2008 hatten die Verteidigungsminister der NATO gemäß geleakter Dokumente beschlossen, Drogennetzwerke als „legitime Ziele“ der Isaf-Truppen zu behandeln, da die Aufständischen „nicht besiegt werden, ohne den Drogenhandel zu unterbinden“. Die Dokumente aus den Jahren 2009 bis 2011, also der Amtszeit von US-Präsident Barack Obama, die aus dem Bestand von Edward Snowden stammen, belegen nach Presseangaben, „auf welch dünnen und teils willkürlich anmutenden Grundlagen die Streitkräfte Verdächtige für gezielte Tötungen nominierten.“ Bei der Exekution von der Luft aus komme es auch zu Verwechslungen und Irrtümern, so dass auch unbeteiligte Männer, Frauen und Kinder getötet würden.

- Strategie der „Säuberung“

Im Juni 2009 setzte der damalige US-Verteidigungsminister Robert Gates den Viersternegeneral Stanley McChrystal

als Oberkommandierenden in Afghanistan ein. Dessen neue Strategie stellte die Aufstandsbekämpfung in den Vordergrund. Ein zentraler Baustein hierfür wurden die Todeslisten. McChrystals Nachfolger, General David Petraeus, beschrieb diese Strategie in einem Handbuch, dem bis heute für den Kampf gegen Guerillagruppen gültigen „Field Manual 3-24“, wobei die erste von drei Stufen als „Säuberungs“-Phase beschrieben wird, wonach die Führungsriege des Gegners geschwächt werden soll. Im August 2010 berichtete Petraeus vor Diplomaten in Kabul, dass mindestens 365 Kommandeure der Aufständischen in den letzten drei Monaten ausgeschaltet worden seien. Die von der Presse ausgewerteten Unterlagen ermöglichen erstmals einen systematischen Blick auf die „Joint Prioritized Effects Lists“ (JPEL). Bei der Abwägung der Vor- und Nachteilen einer Aufnahme auf die Todesliste spielten auch Erwägungen der Abschreckung eine Rolle. Einer Aufnahme in die Liste ging, so die Presseberichte, ein mitunter monatelanger Prozess voraus, bei dem Informationen aus abgehörten Telefonaten, Berichten von Informanten, Fotos usw. ausgewertet wurden. Die Entscheidung über die Listung eines Verdächtigen wurde vom jeweiligen Isaf-Regionalkommandeur getroffen.

Teilweise wurden JPEL-Personen auch nur zur Beobachtung oder Festnahme ausgeschrieben. Gemäß den Snowden-Dokumenten gelang mit Atta Mohammed Noor 2010 sogar ein Gouverneur in Nordafghanistan auf die Liste, jedoch nur, um mehr Informationen über ihn zu sammeln. Aus einem britischen Dossier vom Oktober 2010 geht hervor, dass die Suche nach Telefonsignalen der Taliban „zentral für den Erfolg von Operationen“ war. Hierzu suchten „Predator“-Drohnen und britische Eurofighter rund um die Uhr mit Sensoren die Funksignale nach bekannten, den Taliban zuzuordnenden Mobiltelefonnummern ab. Zur Identifikation von Personen wurden außerdem Stimmprofile abgespeichert und zugeordnet. Die Angriffe führten dazu, dass die Taliban ihre Kämpfer anwiesen, keine Handys mehr zu benutzen.

- Beschwichtigen, Beteiligen und Bremsen

Deutsche Stellen geben seit Jahren Mobilfunknummern von deutschen Extremisten, die sich am Hindukusch aufhalten, an US-Stellen weiter, verbunden mit der Behauptung, für gezielte Tötungen sei das Anpeilen der Telefone viel zu ungenau. Aus einem geleakten Dokument von 2010 geht jedoch hervor, dass sowohl Eurofighter als auch die Drohnen die Möglichkeit haben, „ein bekanntes GSM-Telefon zu lokalisieren“. Aktive Handys dienten den Spezialeinheiten demnach als präzise Peilsender. Deutschland ist am Hindukusch neben u. a. auch Italien, Spanien, Belgien, Frankreich, Schweden und Norwegen Mitglied der Abhörgemeinschaft der „14 Eyes“, der 14 Augen. Diese Länder betreiben in Afghanistan eine eigene technische Plattform mit dem Codenamen „Center Ice“ für die Überwachung und den Austausch von Daten. Diese Austausch bezog sich gemäß einer NSA-Präsentation aus dem Jahr 2009 nicht nur auf Handygespräche, sondern auch auf Informationen zu Zielen.

Der BND räumte die Weitergabe von Mobilfunknummern via „Center Ice“ ein, bestritt aber, dass diese zur Zielerfassung von Drohnen taugen. Zudem würden keine Daten weitergegeben, wenn die „schutzwürdigen Interessen der/des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen“. Seit 2005 lieferten die Deutschen zudem keine Informationen mehr, mit denen Profile für den Zugriff aufgebaut werden können. Die Zurückhaltung der Deutschen führte scheinbar zu Friktionen mit den USA. Wollte das von der Bundeswehr geführte Regionalkommando Nord einen Verdächtigen für die JPEL nominieren, musste erst eine detaillierte Akte mit Beweisen zum Einsatzkommando nach Potsdam und schließlich ans Ministerium geschickt werden. Als Kriterium für die Aufnahme galt, dass die Zielperson an Anschlägen beteiligt gewesen, sie angeordnet oder vorbereitet haben musste. Mehrfach drängten die Deutschen darauf, Verdächtige wieder zu streichen. Im September 2010 entfielen nur 11 der 744 Ziele auf das von den Deutschen militärisch kontrollierte Nordafghanistan. 2010 wurde der deutsche Staatsangehörige Bünjamin E. aus Wuppertal in Waziristan Opfer eines US-amerikanischen Drohnenangriffs. Mobilfunknummern aus Deutschland sollen dabei eine wichtige Rolle gespielt haben. Der Sachverhalt wurde nie genau aufgeklärt. Das Bundeskriminalamt reicht seit längerem keine Daten mehr weiter, die für den gezielten Einsatz von Drohnen eingesetzt werden könnten. General Ramms erklärte: „Wir Deutschen haben einen Stabilisierungseinsatz geführt und die Amerikaner einen Krieg.“

Seit Anfang Januar besteht kein offizielles Isaf-Militärmandat mehr. Die NATO-Truppen sind weitgehend abgezogen. Eine neue Regierung wurde gewählt. Die Taliban sind weiterhin sehr weitgehend handlungsfähig – nicht nur militärisch. Eine CIA-Studie aus dem Jahr 2009 kommt schon zu dem Ergebnis, dass die gezielte Tötung in Afghanistan wegen der zentralen, aber flexiblen Führung der Taliban wenig Erfolg gebracht habe: „Die Taliban haben eine hohe Fähigkeit, ausgeschaltete Führer zu ersetzen.“ Drohnen werden als Mittel zur Tötung von Menschen vom US-Militär seit Jahren genutzt. Einsätze sind dokumentiert in Afrika, im Jemen, in Afghanistan und Pakistan.

- Rechtliche Konsequenzen?

Die Veröffentlichung der vertraulichen Dokumente veranlassten die Menschenrechtsorganisation Reprieve, juristische Schritte gegen die britische Regierung vorzubereiten. Besonders relevant sei insofern, dass sich auf den Listen Pakistaner befinden, die sich in Pakistan aufhielten, so die Reprieve-Anwältin Jennifer Gibson: „Die britische Regierung hat wiederholt beteuert, dass sie keine pakistanische Ziele angreift und dort keine Luftschläge ausführt.“ Es sei rechtlich äußerst problematisch, dass der „Krieg gegen den Terror“ faktisch mit dem „Krieg gegen Drogen“ verschmolzen worden sei. Isaf wollte zu den Dokumenten aus „operativen Sicherheitserwägungen“ keine Stellungnahme abgeben. Isaf-Einsätze entsprächen internationalem Recht.

In Artikel 102 Grundgesetz heißt es: „Die Todesstrafe ist abgeschafft.“ Der BND versieht seine ins Ausland übermittelten Datensätze mit dem „Drohnen-

Paragraf" genannten Zusatz, dass diese nicht als „Grundlage oder Begründung für eine Verurteilung zum Tode verwendet werden (dürfen). Eine Verwendung zum Zwecke des Einsatzes körperlicher Gewalt ist nur zulässig, solange und soweit ein gegenwärtiger Angriff vorliegt oder unmittelbar droht."

Die Einsätze werden durch Infrastruktur in Deutschland unterstützt. Die Bundesregierung reagiert auf solche Berichte mit der Erklärung, sie habe keine eigenen Erkenntnisse. Am 31.12.2014 erklärte die Bundesanwaltschaft, dass sie vorerst wegen der deutschen Beteiligung an der Sammlung von Daten zur gezielten Tötung in Afghanistan nicht ermittelt: „Bislang liegen keine zureichenden tatsächlichen Anhaltspunkte für eine in der Zuständigkeit der Bundesjustiz fallende Straftat vor". Die frühere Bundesjustizministerin Sabine Leutheusser-Schnarrenberger erklärte, das gezielte Töten Verdächtiger ohne irgendeine Angriffshandlung sei nicht gedeckt, insbesondere bei Nichtkämpfenden, etwa Drogendealern. Die deutsche Zuarbeit werfe rechtliche Fragen auf, die „mit Blick auf künftige Kampfeinsätze unbedingt geklärt werden sollten" (Appelbaum/Gebauer/Koelbl/Poitras/Repiski/Rosenbach/Stark, Obamas Listen, Der Spiegel 1/2015, 80-83; Ex-Nato-General bestätigt deutsche Mithilfe an Todeslisten, www.sueddeutsche.de 30.12.2014, Leyendecker/Käppner, Kill M., SZ 31.12.2014/01.01.2015, 7; Taliban-Tötung straflos, SZ 02.01.2015, 6).

Indonesien

„Jungfrauentest" bei Beamtinnen soll abgeschafft werden

Unverheiratete Beamtinnen in Indonesien müssen bisher vor ihrer Einstellung einen Jungfrauentest über sich ergehen lassen. Diese Untersuchungen sollen künftig abgeschafft werden. Das versprach Innenminister Tjahjo Kumolo kurz vor Weihnachten 2014. Die Praxis war im November 2014 öffentlich geworden, als die Menschenrechtsgruppe Human Rights Watch solche Tests bei Polizistinnen in Indonesien anprangerte. Indonesien ist das Land mit der größten muslimischen Bevölkerung der Welt. Die Gesellschaft ist zwar liberal, offiziell sind sexuelle Beziehungen vor der Ehe aber tabu. Der Minister verwarf die Tests aber nicht etwa als diskriminierend gegen Frauen. Vielmehr meinte er, die Frauen könnten ihr Jungfernhäutchen auch anders als durch Sex verloren haben: „Wenn eine Frau keine Jungfrau mehr ist, kann das verschiedene Gründe haben, einen Sturz zum Beispiel. Es wäre schade, wenn die Frau wegen eines nicht bestandenen Tests nicht aufgenommen wird, wenn sie sonst kompetent ist" (Indonesien schafft Jungfrauentest für Beamte ab, www.focus.de 23.12.2014).

Technik-Nachrichten

NSA soll hinter Supervirus „Regin" stecken

Experten der russischen IT-Sicherheitsfirma Kaspersky glichen den in Snowden-Unterlagen gefundenem Code einer Schadsoftware namens „QWERTY" mit eigenen Schadprogrammfunden ab und fanden dabei klare Übereinstimmungen mit einer elaborierten Cyberwaffe, die seit November 2014 international Schlagzeilen macht. Damals hatten sowohl Kaspersky als auch die US-Sicherheitsfirma Symantec erstmals über den Fund eines Cyberwaffensystems berichtet, das sie „Regin" tauften. Laut Kaspersky war die Schadsoftware damals schon mehr als zehn Jahre im Einsatz und war gegen Ziele in mindestens 14 Ländern eingesetzt worden – neben Deutschland, Belgien und Brasilien gehörten dazu auch Indien und Indonesien. Symantec sprach von einer „hochkomplexen" Bedrohung. Viele Angriffsziele stammten aus dem Telekommunikationssektor, andere aus den Bereichen Energie und Fluggesellschaften. Beide Unternehmen beschrieben „Regin" in Superlativen. Es handele sich um die gefährlichste Cyberwaffe seit „Stuxnet" – der berüchtigten Schadsoftware zum Angriff auf das iranische Atomprogramm.

Kaspersky-Forschungschef Costin Raiu erklärte: „Wir sind sicher, dass wir hier das Keylogger-Modul von ‚Regin' vor uns uns haben. Nach unserer technischen Analyse ist ‚QWERTY' identisch mit dem Plugin 50251 von ‚Regin'". QWERTY bezeichnet die Anordnung auf englischen Tastaturen. Ein Keylogger ist ein Programm, das alle Tatstatureingaben mitschneiden kann – beispielsweise Passwörter, E-Mails, Textdokumente – und sie dann unbemerkt an seinen Urheber schickt. Zudem lasse sich daraus ablesen, dass es sich bei Regin offenbar um eine gemeinsame Angriffsplattform verschiedener Institutionen aus verschiedenen Ländern handele.

Die neue Analyse ist ein eindeutiger Beleg dafür, dass es sich bei Regin um die Cyber-Angriffsplattform des „Five Eyes"-Verbunds handelt, also der Geheimdienste der USA, Großbritanniens, Kanadas, Neuseelands und Australiens. Kaspersky äußert sich wie auch Symantec nicht direkt zu den mutmaßlichen Urhebern von Regin. An der Herkunft der Software kann es aber nun kaum noch Zweifel geben. Regin war auch auf den Rechnern des belgischen Telekommunikationsunternehmens Belgacom am Werk. Belgacom war ein Angriffsziel des britischen GCHQ, worüber schon im Sommer 2013 berichtet wurde. Ronald Prins, Chef des niederländischen Sicherheitsunternehmens Fox IT, das unter anderem den Belgacom-Angriff analysiert

hatte, erklärte schon im November 2011, Regin sei offenkundig ein Werkzeug von NSA und GCHQ. Weitere weichere Indizien sprechen dafür, dass „Regin" ein „Five Eyes"-Werkzeug ist:

- Im Code von QWERTY und Regin finden sich zahlreiche Verweise auf die im Commonwealth beliebte Sportart Kricket.
- Es gibt viele Übereinstimmungen mit einem Cyberwaffen-System, das die Geheimdienste selbst in den Snowden-Dokumenten „Warriorpride" nennen.
- Auch die bislang bekannten Angriffsziele passen zu den politischen Überwachungsaufträgen der Five Eyes, wie sie aus dem Archiv des Whistleblowers hervorgehen.

Der Vize-Direktor des Bundesamts für Sicherheit in der Informationstechnik (BSI), Andreas Könen, bestätigte Ende Dezember 2014: „Wir haben das nachvollzogen, es gibt eindeutige Übereinstimmungen." Die österreichische Zeitung „Der Standard" berichtete unter Berufung auf anonyme Quellen, dass auch im Netzwerk der Internationalen Atomenergiebehörde IAEA Schadcode der Regin-Familie nachgewiesen worden sei. Die „Bild"-Zeitung berichtete zudem über eine Regin-Infektion bei einer Mitarbeiterin des Europareferats im Bundeskanzleramt. Diese habe allerdings den Privatrechner der Frau betroffen. In deutschen Regierungsnetzen sei, so das BSI, Regin bislang nicht nachgewiesen worden, hieß. Mit weiteren Funden von Regin ist nach Lage der Dinge wohl zu rechnen. Allein bei Kaspersky hat man gemäß Raiu den Schadcode inzwischen bei 27 internationalen Unternehmen, Regierungen und Privatpersonen nachgewiesen (Rosenbach/Schmundt/Stöcker, Experten enttarnen Trojaner „Regin" als NSA-Werkzeug, www.spiegel.de, 27.01.2015; Martin-Jung/Tandriverdi, NSA soll hinter Supervirus stecken, SZ 28.01.2015, 20).

Biometrieauthentisierung mit hochauflösenden Fotos kompromittiert

Jan Krissler, Forscher an der Technischen Universität (TU) Berlin, bekannt unter dem Namen „starbug", demonstrierte am 27.12.2014 beim 31. Chaos Communication Congress (31C3), wie einfach biometrische Authentifizierungssysteme auszuhebeln sind. Biometrische Merkmale werden auch als Beweismittel für den Tatbeitrag eines Menschen an einer Straftat verwendet. Um einen Fingerabdruck zu fälschen, reicht ihm ein hochauflösendes Foto, zum Beispiel eines von den Händen von Bundesverteidigungsministerin Ursula von der Leyen. Das zu besorgen, ist für einen Fotografen kein größeres Problem. Schon ein Objektiv mit einer Brennweite von zweihundert Millimetern reicht, um geeignete Bilder selbst aus sechs Metern Entfernung zu machen. Der Abdruck kann dann für eine Attrappe genutzt werden. Krissel kündigte an, von der Leyens Fingerabdruck demnächst als dreidimensionale Folie zu veröffentlichen. Bereits vor einigen Jahren hatte Krissler einen künstlichen Fingerabdruck aus dem Daumenabdruck von Wolfgang Schäuble hergestellt, der damals Innenminister war. Schäuble hatte seinen Abdruck auf einem Wasserglas auf einer Konferenz hinterlassen, der als Grundlage für eine Reproduktion genügte.

Andere Sicherheitssysteme verwenden als biometrisches Merkmal die Iris oder das Gesicht. Auch die sind mit guten Fotos problemlos zu täuschen. Mitunter reicht es, Fotos mit hoher Auflösung (1.200 dpi) auszudrucken und vor den Irisscanner beziehungsweise die Kamera zu halten. Krissler zeigt das am Beispiel der Software KeyLemon. Mehr als 1000 Euro hat sein Team ausgegeben für diesen professionellen Iris-Scanner. Die entsperrt einen Rechner auf Wunsch nur nach Gesichtsabgleich, fällt aber auch auf ein Foto herein. Der Biometrieforscher wies darauf hin, dass ein Angreifer solche Fotos nicht selbst machen muss. Von vielen Menschen gibt es geeignete Bilder im Netz. Von Politikern wie Angela Merkel etwa finden sich dort qualitativ hochwertige Wahlplakate als exzellente Vorlage. Der Ausdruck muss nur gut genug sein.

Noch leichter wird es für den Angreifer, wenn dieser auf die Kamera des Smartphones seines Opfers zugreifen kann. Unter Laborbedingungen hat es Krissler geschafft, mithilfe einer präparierten App ein Bild des Fingers zu machen, als das Opfer den Finger nur kurz über das Gerät hielt, mit er eine funktionierende Fingerabdruckattrappe herstellte. Heutige Smartphonekameras bieten zum Teil 13 Megapixel Auflösung und mehr. Sogar die schwächeren Frontkameras werden immer besser, um sie für Selfies und Videotelefonie nutzen zu können.

Für einen weiteren Trick erhielt Krissler beim 31C3 großen Applaus: In Fotos, die mit der Frontkamera gemacht werden, spiegelt sich das Display des Smartphones in der Pupille des Nutzers. Reicht die Auflösung, kann Krissler im Zoom erkennen, wie der Finger des Nutzers die PIN eingibt. „Videos sind in der Regel weniger hoch aufgelöst. Deswegen ist es aus Sicht eines Angreifers sinnvoller, mehrere Fotos pro Sekunde zu machen. Oder man löst die Kamera immer dann aus, wenn das Gyroskop im Smartphone die PIN-Eingabe, also das Tippen auf dem Display registriert." Noch sei das ein wenig in die Zukunft gedacht, weil die meisten Frontkameras nur mit 1,2 bis zwei Megapixel auflösen. Aber dass es prinzipiell funktioniert, hat Krissel bereits zusammen mit Tobias Fiebig und Ronny Hänsch in einer Forschungsarbeit mit dem Titel Security Impact of High Resolution Smartphone Cameras beschrieben.

Noch nicht ausprobiert hat Krissler folgenden Angriff, den er aber technisch für machbar hält: „Man kann sich auch Kontaktlinsen bemalen lassen, das ist weniger auffällig, als ein Foto vor eine Kamera zu halten." Solche Irislinsen gibt es bereits – teuer – zu kaufen. „Man kann die Strukturen einer Iris sehr fein nachmalen. Ich bin relativ sicher, dass es funktionieren würde. Es gibt Holografie, die auf eine definierte Wellenlänge ausgerichtet ist. Man sieht das Hologramm also nur, wenn man es aktiv mit Licht dieser Wellenlänge beleuchtet." Eine entsprechend präparierte Kontaktlinse würde in Weißlicht ganz normal aussehen. Im typischen Infrarotlicht eines Irisscanners dagegen würde das Hologram auf der Linse sichtbar werden und die Iriserkennung austricksen können. „Man kann die Kontaktlinse natürlich auch mit Infrarotfarbe bedrucken, das ist noch viel einfacher! Die ist im normalen Licht nicht zu sehen, aber im Infrarotlicht des Scanners."

Manche Irisscanner lassen sich nicht ganz so einfach überlisten. Sie setzen ein Lebenszeichen voraus, nicht nur ein unbewegtes Bild. Oft reicht ihnen allerdings ein Blinzeln. Krissler demonstrierte dies am Beispiel von KeyLemon: Er legt dem Programm wiederum ein Foto vor, schwenkt dann aber einmal kurz mit einem Stift über die Augen. Die sind dadurch kurz bedeckt und KeyLemon interpretiert das als Blinzeln.

Zwar sind einige der Angriffsszenarien nicht alltagstauglich, weil es z. B. neben der biometrischen noch andere Überprüfungen gibt, bevor jemand authentifiziert wird. Evtl. muss man den Rechner oder das Smartphone eines Opfers in seinen Besitz bringen, um die Iriserkennung darauf aushebeln zu können. Aber die biometrischen Verfahren für sich genommen lassen sich laut Krissler fast alle austricksen – vor allem, wenn man genug Zeit und Geld hat: „Ich glaube nicht, dass man sie sicher machen kann. Allenfalls sicherer.“ Er rät den Herstellern solcher Technik, die Attrappenerkennung zu verbessern oder auf Merkmale auszuweichen, an die Unbefugte nicht so einfach kommen können, wie z. B. Venenmuster oder den Augenhintergrund (Boie, Mit anderen Augen, SZ 29.12.2014, 6; Beuth, Diese Augen können lügen, www.zeit.de 28.12.2014).

Studie: Algorithmen berechnen Persönlichkeit besser als Menschen

Im Wissenschaftsmagazin PNAS (online) führte ein Forschungsteam um Wu Youyou und Michal Kosinski von der University of Cambridge den Nachweis, dass Computer regelmäßig die Persönlichkeit von Menschen besser erfassen können als deren soziales Umfeld, also besser als KollegInnen, Familie und Freunde. Die Forschenden ermittelten mit einem online gestellten Standardfragebogen die Persönlichkeitseigenschaften von mehr als 86.000 ProbandInnen gemäß dem Big-Five-Modell der Psychologie.

Gemäß diesem Ansatz lässt sich der Charakter eines Menschen damit beschreiben, wie stark fünf Eigenschaften ausgeprägt sind: Neurotizismus, Extroversion, Verträglichkeit, Gewissenhaftigkeit und Offenheit für neue Erfahrungen In einem weiteren Schritt mussten dann Facebook-Freunde dieser Versuchspersonen mithilfe eines vereinfachten Fragebogens ebenfalls Big-Five-Profile der ursprünglichen ProbandInnen erstellen. Per Rechner wurden sodann die Facebook-Likes der Studiengruppe erfasst, ausgewertet und mit in anderen Studien zuvor entwickelten Algorithmen jeweils zu einem Profil verdichtet. Dabei zeigte sich im Durchschnitt eine leicht bessere Übereinstimmung mit dem Selbsttest der ProbandInnen als bei der Beurteilung durch deren soziales Umfeld.

Die Ergebnisse bestätigen frühere Studien, wonach sich aus den durch die Likes offenbarten Vorlieben Persönlichkeitseigenschaften ablesen lassen: Wer angibt, gerne zu tanzen und auf Partys zu gehen, der ist vermutlich eher extrovertiert. Wer gerne wissenschaftliche Vorträge hört und neue Kunst besichtigt, ist wahrscheinlich offen für Erfahrungen. Ein neues Ergebnis ist, dass Computer solche Daten verlässlicher auswerten als Menschen – mit einer Ausnahme: Ehepartner beurteilten sich gegenseitig – noch – um einen Tick besser. Es ist aber zu vermuten, dass Computer noch besser werden, wenn sie mehr Datenmaterial erhalten. Womöglich entwickeln die Rechner dabei weitere diagnostische Fähigkeiten. Die Forschenden aus Cambridge zeigen in der vorliegenden Studie, dass die Algorithmen besser als Menschen voraussagen konnten, ob die ProbandInnen etwa Drogen nehmen, depressiv oder bei schlechter Gesundheit sind. Entsprechend vielfältige neue Anwendungen lassen sich vorstellen – von der Werbung über das automatische Screenen von Bewerbenden für Personalabteilungen bis hin zur Partnersuche (Weber, Du bist, was du liebst, SZ 13.01.2015, 16).

Soziale Medien

Twitter spioniert Apps aus

Am 26.11.2014 teilte der Nachrichtendienst Twitter in einem Blogeintrag mit, dass er künftig auf einem Smartphone installierte Apps aufspüren möchte, um mehr über die Interessen seiner Nutzenden herauszufinden und auf dieser Basis gezielte Werbung zu platzieren: „Wir sammeln und aktualisieren gelegentlich die Liste von Apps, die auf deinem Mobilgerät installiert sind, so dass wir Inhalte liefern können, die dich interessieren könnten.“ Nicht ausgewertet werde, wie die Nutzenden die Programme auf ihren Smartphones nutzen. Ziel der Änderung ist es, die Aktivitäten der Mitglieder und die Werbeeinnahmen zu steigern (Twitter spürt künftig Ihren Apps nach! www.bild.de 27.11.2014).

Uber will alles wissen

Dem Fahrdienstvermittler Uber wird vorgeworfen, in seiner App für Android-Geräte unnötig viele Daten einzusammeln. Ein US-amerikanischer Software-Experte kam bei einer Anwendungsanalyse zu dem Ergebnis, dass Uber neben dem Zugang zu Kamera, Kontakten und Ortsdaten viele weitere Informationen bis hin zum Batteriestand abfragt. Uber erklärte, dies sei für den Betrieb nötig. Informationen über die Namen der umliegenden WLAN-Netze dienten der präzisen Bestimmung des Nutzenden für die Abholung. Der Zugang zur Kamera sei erforderlich für Profilfotos und eine Funktion zum schnellen Einlesen von Kreditkarten-Informationen. Mit dem Zugriff auf die Telefon-Funktion könne

die KundIn die Fahr-Anbieterin anrufen. In einem Blogeintrag wurde ein Teil des Programmcodes veröffentlicht, der den Eindruck erweckt, dass die Uber-App auch Informationen über Telefon-Anrufe und SMS-Verkehr überträgt (Datensammelei per App: Sicherheitsexperte vergleicht Uber mit der NSA, www.spiegel.de, 27.11.2014)

Rechtsprechung

EuGH

Datenschutzrecht ist bei privater Videoüberwachung anwendbar

Der Europäischer Gerichtshof (EuGH) urteilte am 11.12.2014, dass auch Privatpersonen das europäische Datenschutzrecht, hier die Datenschutz-Richtlinie (EU-DSRL) beachten müssen, wenn sie z. B. aus Furcht vor Kriminellen ihr Haus mit einer Kamera überwachen und dabei öffentlicher Grund wie etwa der Gehweg oder die Straße gefilmt werden (C-212/13). Im Fall des Tschechen František Ryneš hatte dieser nach mehreren Angriffen auf sein Haus mit einer Kamera seinen Eingang, die Straße davor und den Eingang des gegenüberliegenden Hauses überwacht. Bei der nächsten Attacke, bei der mit einer Schleuder eine Fensterscheibe zu Bruch geschossen wurde, erfasste er damit zwei Verdächtige und meldete diese der Polizei. Einer der Verdächtigten bezweifelte beim tschechischen Amt für den Schutz personenbezogener Daten, ob die Überwachung rechtmäßig ist. Das Amt befand, dass Ryneš gegen die Datenschutz-Vorschriften verstoßen hat, weil die Verdächtigen ohne ihre Einwilligung überwacht wurden, und verhängte gegen ihn eine Geldbuße.

Vom Anwendungsbereich der EU-DSRL ausgenommen sind Maßnahmen der Datenverarbeitung, die eine Person „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ vornimmt. Der EuGH entschied, dass die Überwachung in diesem Fall nicht dazu zählt, auch wenn Ryneš sein Leben, seine Gesundheit und sein Eigentum schützen wollte. Die Ausnahme sei eng auszulegen. Die Datenverarbeitung dürfe „dann ohne die Einwilligung der betroffenen Person erfolgen, wenn sie zur Verwirklichung des berechtigten Interesses des für die Verarbeitung Verantwortlichen erforderlich ist“. Um Erlaubnis gefragt werden muss gemäß dem Urteil auch nicht, wenn dies „unmöglich ist oder unverhältnismäßigen Aufwand erfordert“. Und die EU-Mitgliedstaaten dürften eigene Regeln erlassen, wenn es um die Verhütung oder Aufklärung von Straftaten gehe.

In Deutschland gilt § 6b des Bundesdatenschutzgesetzes (BDSG), das die EU-DSRL von 1995 umsetzt. Die deutschen Datenschutzaufsichtsbehörden haben eine 20seitige „Orientierungshilfe“ veröffentlicht, die genau auflistet, was Hausbesitzer alles beachten müssen, bevor sie eine Kamera anschrauben (Europäischer Gerichtshof: Datenschutz gilt auch für private Videoüberwachung, www.heise.de 11.12.2014; EuGH PM v. 11.12.2014, Die Richtlinie zum Schutz personenbezogener Daten ist auf die Videoaufzeichnung mit einer Überwachungskamera anwendbar, die von einer Person an ihrem Einfamilienhaus angebracht wurde und auf den öffentlichen Straßenraum gerichtet ist; Düsseldorfer Kreis – Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“, www.baden-wuerttemberg.datenschutz.de).

EuGH

Informationeller Schutz für homosexuelle Flüchtlinge

Der Europäische Gerichtshof (EuGH) in Luxemburg hat mit Urteil vom 02.12.2014 klargestellt, dass die homosexuelle Ausrichtung von Flüchtlingen als Asylgrund geprüft werden darf (C-148/13; C-149/13; C-150/13). Tests, Videos mit sexuellen Handlungen der Flüchtlinge und zudringliche Befragungen verstoßen jedoch gegen die Grundrechtecharta der EU und sind nicht zulässig.

Homosexuelle werden in vielen Ländern weltweit diskriminiert, verfolgt und bestraft. In einigen Ländern wie Saudi-Arabien, Sudan, Iran oder Jemen steht sogar die Todesstrafe auf gleichgeschlechtliche Liebe. Seit November 2013 ist durch den EuGH anerkannt, dass wegen Homosexualität in der EU Asyl beantragt werden kann. In einem weiteren Urteil hatte der EuGH 2012 im Hinblick auf religiöse Verfolgung entschieden, dass Betroffenen nicht zuzumuten sei, ihr religiöses Bekenntnis geheim zu halten. Dies gilt auch für die sexuelle Orientierung. Nach dem nun gefällten Urteil sind die nationalen Behörden berechtigt, die Asylbewerber zu befragen, um die behauptete sexuelle Ausrichtung zu prüfen. Doch schon Fragen zu Einzelheiten sexueller Praktiken verstoßen dem EuGH zufolge gegen die Grundrechtecharta der Europäischen Union (EU) – insbesondere gegen das Recht auf Achtung des Privat- und Familienlebens. Das Gericht lehnte den Vorschlag, den einige Asylbewerber selbst gemacht haben, ab, mittels eigener homosexueller Handlungen, mit Hilfe von Tests oder mit Videoaufnahmen intimer Handlungen die sexuelle Orientierung zu beweisen. Dadurch werde „die Würde des Menschen verletzt“. Darüber hinaus sei die Beweiskraft solcher Maßnahmen fraglich. Es könnte andere Antragsteller dazu bewegen, ebenfalls solche Beweise zu beschaffen und letztlich bestünde das Risiko, dass Behörden

so etwas von Flüchtlingen sogar verlangen würden.

Der EuGH weist auf den sensiblen Charakter von Informationen hin, die die Sexualität einer Person betreffen. Das Zögern einer Person, intime Aspekte ihres Lebens zu offenbaren, könne dazu führen, dass sie ihre Homosexualität nicht sofort angibt. Allein daraus dürfe jedoch nicht geschlossen werden, dass sie unglaubwürdig ist. Außerdem dürften die Behörden bei ihren Fragen nicht von „stereotypen Vorstellungen in Verbindungen mit Homosexualität" ausgehen. Ein Asylbewerber, der nicht in der Lage sei, entsprechende Fragen zu beantworten, sei deshalb noch nicht unglaubwürdig. Die Richter folgen einem Gutachten der Generalanwältin Eleanor Sharpston vom Gerichtshof vom Juli 2014. Sharpston hatte festgestellt, dass „bestimmte Prüfungsmethoden wie medizinische oder pseudo-medizinische Untersuchungen, zudringliche Befragungen oder die Anforderung des Nachweises sexueller Aktivitäten mit der Charta der Grundrechte unvereinbar" seien. Zu solchen Untersuchungen gehört die „Phallometrie", die tschechische Behörden bis 2010 anwandten. Dabei wurden männlichen Asylbewerbern Pornofilme für Heterosexuelle gezeigt, während der Blutfluss im Penis gemessen wurde. Die Grundrechteagentur der Europäischen Union hatte dieses Vorgehen als entwürdigend kritisiert. Bekannt geworden war der Einsatz des Tests, nachdem das Schleswig-Holsteinische Verwaltungsgericht 2009 die Rückführung eines Asylbewerbers aus dem Iran nach Tschechien mit Hinweis auf die Behandlung dort verhindert hatte.

Anlass für die aktuelle Entscheidung des EuGH waren drei Anträge von Asylbewerbern aus Uganda, Sierra Leone und Senegal in den Niederlanden. Die drei Flüchtlinge waren in erster Instanz gescheitert, da sie das Gericht nicht von ihrer Homosexualität überzeugen konnten. Einer von ihnen hatte daraufhin angeboten, sich einem Test zu unterziehen, ein anderer wollte ein Video präsentieren, das ihn beim Sex mit einem Mann zeigte. Das war von den Behörden abgelehnt worden. Der niederländische Staatsrat wollte vom EuGH nun wissen, welche Maßnahmen die in der Grundrechtecharta der EU garantierten Rechte verletzen würden – und ob dies nicht bereits der Fall sei, wenn dem Asylbewerber nur Fragen gestellt würden.

In ihrem Gutachten hatte Sharpston festgestellt, dass sich die Anerkennung als Asylbewerber auf die Frage zu konzentrieren habe, ob der Antragsteller glaubwürdig sei. Es müsste geprüft werden, ob sein Vorbringen plausibel und kohärent ist. „Eingriffsintensive und erniedrigende Methoden" wie die Phallometrie würden jedoch „die Rechte auf körperliche und geistige Unversehrtheit und auf Privatleben" verletzten. Das Gleiche gelte für „zudringliche Befragungen". Die Gutachterin hatte auch die Vorlage von Foto- oder Videobeweisen für sexuelle Praktiken abgelehnt.

In der deutschen Praxis holte schon zuvor das zuständige Bundesamt für Migration und Flüchtlinge (BAMF) keine Gutachten zur sexuellen Orientierung mehr ein. Manfred Bruns vom Verband der Lesben und Schwulen weist aber darauf hin, dass in früheren Zeiten ähnliche Prüfungen üblich waren, nämlich, ob bei einem Flüchtling eine „irreversible, schicksalhafte homosexuelle Prägung" vorliege. Marei Pelzer, Juristin bei Pro Asyl, begrüßte das Urteil: „Der EuGH hat klargestellt, dass bestimmte diskriminierende Verfahren, die gegen Grundrechte verstoßen, nicht mehr zulässig sind". Damit stehen die Behörden zwar immer noch vor dem Problem, dass bei Asylverfahren die Regel ist: Dokumente und andere Belege für eine Verfolgung fehlen – das Beweismittel ist die Aussage des Asylbewerber. Und diese Aussage muss eingeschätzt und bewertet werden. Pelzer: „Das aber darf nach dem EuGH-Urteil in Zukunft nicht mehr auf diskriminierende Art und Weise stattfinden" (Janisch, Asylrecht Homosexueller in Europa gestärkt, SZ 03.12.2014, 7; Schulte von Drach, Mehr Schutz für homosexuelle Flüchtlinge, www.sueddeutsche.de 02.12.2014).

BVerfG

Antrag auf Zeugenvernehmung von Snowden in Berlin als unzulässig verworfen

Mit Beschluss vom 04.12.2014 erklärte das Bundesverfassungsgericht (BVerfG) die Organklage der Fraktionen „Die Linke" sowie „Bündnis 90/Grünen", von 127 Bundestagsabgeordneten und den beiden Ausschussmitgliedern im NSA-Untersuchungsausschuss Konstantin von Notz und Martina Renner, mit der eine Anhörung von Edward Snowden in Berlin erstritten werden sollte, für unzulässig (2 BvE 3/14). Die beanstandete Weigerung der Bundesregierung wurde als vorläufige Einschätzung angesehen; die keine rechtserhebliche Maßnahme sei, gegen die sich ein Organstreitverfahren richten kann. Der Antrag beträfe kein in Art. 44 Abs. 1 GG wurzelndes Recht der Ausschussminderheit gegenüber dem Untersuchungsausschuss. Es gehe um eine verfahrensrechtliche Überprüfung der Ausschussarbeit im Einzelnen, für die der Bundesgerichtshof (BGH) zuständig sei.

Die Antragsteller machen im Wesentlichen geltend, die Bundesregierung habe in zwei Schreiben von Mai und Juni 2014 ihre – seither aufrecht erhaltene – Weigerung zum Ausdruck gebracht, die Voraussetzungen für eine Zeugenvernehmung von Edward Snowden in Berlin zu schaffen, und damit ihre Pflicht zur Unterstützung des Untersuchungsausschusses aus Art. 44 Abs. 1 GG verletzt. Der NSA-Untersuchungsausschuss habe zudem durch die Ablehnung von Anträgen im Juni und im Juli 2014 sowie durch seine fortgesetzte Verhinderung der Ladung von Edward Snowden nach Berlin seine Pflicht verletzt, dem Untersuchungsauftrag nachzukommen.

Das BVerfG meinte, die bisherigen „Einschätzungen" der Bundesregierung seien nur vorläufiger Natur. Wesentliche Erkenntnisse zum relevanten Sachverhalt lägen nicht vor oder seien jedenfalls nicht gesichert. Dies betreffe etwa die Fragen, ob Edward Snowden im Besitz eines gültigen Passes ist und ob seitens der Behörden der Russischen Föderation eine Ausreise bewilligt oder eine Zustimmung der russischen Behörden zur Zeugenvernehmung vor Ort erteilt würde. Der Bundesregierung läge noch kein konkretes Amtshilfeersuchen des Untersuchungsausschusses vor. Deren Stellungnahme sei unverbindlich, von ihr läge noch keine Entscheidung über die Behandlung eines Amtshilfeersuchens vor, die rechtliche Außenwirkung entfalte. Deshalb seien die Antragsteller

in ihren verfassungsrechtlich garantierten Rechten nicht berührt.

Bei den Anträgen auf Vorladung von Edward Snowden habe es sich nicht um Beweisanträge, sondern um Verfahrensanträge zur Ausgestaltung der weiteren Arbeit des Untersuchungsausschusses gehandelt. Für einen Beweisantrags müsse das Beweismittel hinreichend präzise benannt werden, was nicht erfolgt sei. Gemäß § 36 Abs. 1 des Untersuchungsausschussgesetzes (PUAG) ist für Streitigkeiten nach dem Untersuchungsausschussgesetz der BGH zuständig. Diesem käme keine verfassungsrechtliche Zuständigkeit zu, sondern allein die verfahrensrechtliche Überprüfung der Ausschussarbeit im Einzelnen, zum Beispiel bezüglich der Erhebung bestimmter Beweise, der Verlesung von Schriftstücken oder der Herausgabepflicht von Gegenständen. Hier gehe es nicht um einen Streit über die Rechte und Pflichten von Verfassungsorganen in einem Verfassungsrechtsverhältnis. Es gehe nämlich nicht um das aus Art. 44 Abs. 1 GG abzuleitende Beweiserzwingungs- und Beweisdurchsetzungsrecht der qualifizierten Minderheit im Ausschuss. Die Bestimmung des Vernehmungsortes und des Zeitpunktes der Vernehmung betreffe die Modalitäten des Vollzugs eines bereits ergangenen Beweisbeschlusses. Hierüber entscheide grundsätzlich die jeweilige Ausschussmehrheit nach Maßgabe der §§ 17 ff. PUAG und der sinngemäß anwendbaren Vorschriften der Strafprozessordnung. Da dem Antrag auf Zeugenvernehmung von Edward Snowden – in Moskau – seitens des Untersuchungsausschusses durch Erlass eines Beweisbeschlusses entsprochen wurde, sei das Beteiligungsrecht der qualifizierten Minderheit nicht betroffen. Es gehe nur um die einfachrechtliche Frage, ob und wie zur Erreichung des Aufklärungszwecks eine unmittelbare Einvernahme vor dem Untersuchungsausschuss vorzunehmen ist.

Der Vorsitzende des NSA-Untersuchungsausschusses Patrick Sensburg (CDU) bezeichnete die Klageabweisungen als Rückschlag, Klatsche und „Reinfall für die Opposition“. Linke und Grüne wollen nun „alle in Betracht kommenden Möglichkeiten“ prüfen, um doch noch eine Befragung Snowdens in Deutschland zu erreichen – auch den Gang zum BGH (Prantl, Zerkrümelter Parlamentarismus, SZ 13./14.12.2014, 9; Snowden muss nicht in Deutschland aussagen, KN 13.12.2014, 4, PE BVerfG v. 12.12.2014, Antrag im Organstreitverfahren zur Zeugenvernehmung von Edward Snowden in Berlin ist unzulässig).

OLG Koblenz

Löschanspruch bzgl. digitaler Intimfotos nach Trennung

Mit Urteil vom 20.05.2014 entschied das Oberlandesgericht (OLG) Koblenz, dass konsensual angefertigte digitale Sexfotos nach Ende der Partnerschaft auf Aufforderung zu löschen sind (3 U 1288/13) und bestätigte damit das Urteil der Vorinstanz. Das Anfertigen von personenbezogenen Lichtbildaufnahmen ist grundsätzlich nur mit Einwilligung des Abgebildeten zulässig und stellt anderenfalls einen widerrechtlichen Eingriff in das Recht am eigenen Bild als besondere Ausprägung des allgemeinen Persönlichkeitsrechts dar. Eine einmal erteilte Einwilligung entfaltet nach weit verbreiteter Ansicht eine gewisse Bindungswirkung, so dass sie nur unter besonderen Umständen für die Zukunft widerrufen werden kann. Solch besondere Umstände nahm nun das OLG Koblenz für in einer Beziehung erstellte Akt- und Intimfotos nach der Trennung an und sprach der Abgebildeten unter Bestätigung des Widerrufs der Einwilligung einen Anspruch auf Löschung zu.

Der Beklagte, ein Berufsfotograf, hatte im Verlauf seiner Beziehung zur Klägerin mit deren Einwilligung mehrere Intimfotographien und Aufnahmen beim Geschlechtsverkehr erstellt. Nach der Trennung hatte er intime Mails, die die Klägerin an ihn gesendet hatte, in elektronischer Form an die Firmenadresse des heutigen Ehemann der Klägerin weitergeleitet, nicht aber Fotos oder Filme. Die Klägerin begehrte unter Berufung auf ihr Recht am eigenen Bild die Löschung aller sich im unmittelbaren oder mittelbaren Besitz befindlichen elektronischen Vervielfältigungsstücke der damals erstellten Intimaufnahmen. Das OLG bestätigte deren Anspruch auf Löschung als besondere Form der Unterlassungsklage nach §§ 823 Abs. 1, § 1004 Abs. 1 Satz 2 BGB. Die ursprünglich erteilte Einwilligung sei als widerrufen zu erachteten. Zwar habe sich das zur Zeit der Aufnahmen vorliegende Einverständnis der Klägerin auch darauf bezogen, dass der Beklagte die entstandenen Bilder im Besitz haben und über sie verfügen durfte. Doch schließe die Einwilligung deren Widerruf für die Zukunft nicht zwingend aus, wenn eine etwaige Bindungswirkung eines einmal bekundeten Einverständnis im Widerspruch zu schützenswerten Persönlichkeitsrechtsaspekten steht. Ein Widerruf ist möglich, wenn auf einem Wandel der inneren Einstellung basierende veränderte Umstände vorliegen, die ein Festhalten an der in der Vergangenheit erteilten Einwilligung unzumutbar erscheinen lassen.

Derartige veränderte Umstände wurden im vorliegenden Fall angenommen. Die fraglichen Aufnahmen waren aus der Intimität einer Liebesbeziehung heraus entstanden, welcher durch die Trennung die Grundlage entzogen wurde, und nicht primär aus der Ausübung der beruflichen Tätigkeit des Beklagten. Gleichzeitig sei zu berücksichtigen, dass die Abbildungen dem Kernbereich der Persönlichkeit zuzuordnen seien und eine etwaige, dies berücksichtigende Sorgfalt des Beklagten im Umgang mit den Aufnahmen mit Blick auf die vorangegangene Verbreitung per Mail nicht angenommen werden könne. „Allein aus der Existenz“ der Fotos und Filme könne durch deren digitale Speicherung ein Gefahr erwachsen, dass die Daten, etwa durch Hacking, an Dritte gelangen. Die sich aus den veränderten Umständen ergebenden Persönlichkeitsinteressen der Klägerin seien im konkreten Fall höher zu werten als entgegenstehende Rechte des Beklagten aus seinem Eigentumsrecht und der Garantie der allgemeinen Handlungsfreiheit. Schon das Versenden der intimen Mails begründe „durchaus Anlass zu Zweifeln“, dass der Fotograf „mit den Aufnahmen mit der gebotenen größtmöglichen Sorgfalt umgeht“. Selbst wenn man auf dessen Profession als Fotograf und ein insofern bestehendes gesteigertes Interesse an dem künstlerischen Gehalt der Fotos abstellte, könne nichts anderes gelten. Insofern

nämlich sei nicht die künstlerische Betätigung an sich von dem Löschungsbegehren der Klägerin betroffen, sondern allein die Darbietung und Verbreitung der Aufnahmen bzw. deren ausschließliche Verwendung zur Eigenbetrachtung, welche hinter dem tangierten Persönlichkeitsrecht der Klägerin zurücktreten müssten.

Grundsätzlich erstreckt sich die Einwilligung in Intim- oder Aktaufnahmen auch auf die Inbesitznahme und die Verfügung durch den aufnehmenden Dritten. Allerdings kann die Einwilligung mit der Wirkung für die Zukunft widerrufen werden, wenn deren Grundlage nachträglich entfällt, also veränderte Umstände eintreten, durch die eine Bindungswirkung der Einwilligung einer Persönlichkeitsrechtsverletzung gleichkommen würde. Werden Intimfotos auf der Vertrauensbasis einer Liebesbeziehung angefertigt, kann die spätere Trennung einen Löschungsanspruch begründen. Auf Nachfrage stellte der Sprecher des OLG Thomas Henrichs klar, dass das Urteil „keine verkörperten Fotografien" wie Abzüge oder Negative umfasse. Der Löschanspruch beziehe sich auf digitale Dateien, nicht z. B. auf Ausdrucke (Salewski, OLG Koblenz: Während einer Beziehung erstellte Intimfotos müssen nach Trennung gelöscht werden, http://www.it-recht-kanzlei.de 29.09.2014; Hipp, Nackte Festplatte, Der Spiegel 22/2014, 137).

LG Berlin

Einwilligungen für Facebook-App-Zentrum unwirksam

Das Landgericht Berlin hat auf die Klage des Verbraucherzentrale Bundesverbands (vzbv) mit Urteil vom 28.10.2014 ein am 09.09.2013 ergangenes Versäumnisurteil gegen Facebook bestätigt, das feststellt, dass Nutzende des Facebook App-Zentrums nicht ausreichend über die umfassende Datenweitergabe an App-Anbieter informiert werden, weshalb die erteilten Einwilligungen nicht bewusst erfolgen und deshalb rechtswidrig sind (Az. 16 O 60/13).

Facebook bietet in seinem eigenen App-Zentrum die Möglichkeit, zahlreiche Apps von Drittanbietern zu nutzen. Dazu gehören beliebte Spiele wie FarmVille oder Café World, Umfragen oder Ratespiele. Durch Klicken auf den Button „Spiel spielen" oder „An Handy laden" wird die Einwilligung des Nutzers zur umfassenden Datennutzung und -weitergabe unterstellt. Eine Auflistung der Daten, die der App-Anbieter erheben und nutzen will, befindet sich unterhalb des Buttons in kleiner, hellgrauer Schrift. App-Anbieter erhalten danach beispielweise die Erlaubnis, auf den Chat, die Informationen zu Freunden und die persönlichen Kontaktdaten zuzugreifen, sowie auf der Pinnwand des Nutzers zu posten.

Michaela Zinke, Referentin für Datenschutz im Projekt Verbraucherrechte in der digitalen Welt beim vzbv, erläutert die Klage: „Drittanbieter erhalten durch die Einwilligung umfassende Zugriffsrechte auf das Profil und die Kontakte von Facebook-Nutzern, ohne dass sich die Nutzer darüber bewusst sind. Der Nutzer sagt mit dem Klick auf den Button nicht nur ‚Spiel spielen', sondern auch ‚Hier sind alle meine Daten'." Das Urteil des LG Berlin bestätigt, dass eine solche umfassende Datenweitergabe an Dritte nach deutschem Recht eine bewusste und informierte Einwilligung eines Nutzers erfordert, die bei der Betätigung des Buttons „Spiel spielen" oder „An Handy laden" nicht gegeben ist. Das Landgericht Berlin hat dies mit seinem Urteil bestätigt: „Der Kläger weist zu Recht darauf hin, dass die Teilnahme an einem kostenlosen Spiel aus der Sicht des durchschnittlich aufmerksamen Referenzverbrauchers keine Handlung darstellt, deren Folgen einer sorgfältigen Abwägung bedürfen. … Eine ´informierte Entscheidung` zum Datentransfer im Sinne der Datenschutzrichtlinie und § 4 Abs. 1 BDSG geht jedoch damit (mit den Datenverwendungsrichtlinien von Facebook, die Hinweise auf eine Datenübermittlung an Apps geben) nicht einher, weil auch das Klauselwerk keine Informationen über den Zweck der Datenweitergabe enthält und auch nicht enthalten kann, wenn jeder Dritte sich die Verwendung der übermittelten Daten in einem von ihm selbst festgelegten Umfang in seinen Allgemeinen Geschäftsbedingungen vorbehält. … Es handelt sich (bei dem in § 4 Abs. 1 BDSG enthaltenen Verbot der Datenübermittlung) um eine Marktverhaltensvorschrift im Sinne des § 4 Nr. 11 UWG." Das LG stellte weiterhin fest, dass folgende Formulierung eine unangemessene Benachteiligung eines Verbrauchers i. s. v. § 307 BGB ist, die einen Unterlassungsanspruch nach den §§ 1, 4a UKlAG begründet: „Diese Anwendung darf Statusmeldungen, Fotos und mehr in deinem Namen posten". Das Urteil des LG Berlin ist noch nicht rechtskräftig. Der vzbv geht davon aus, dass Facebook Berufung einlegen wird (PM vzbv 07.11.2014, Facebooks App-Zentrum: Lösung zur Einwilligung in Datenweitergabe ist rechtswidrig).

VG Koblenz

Keine Einreisekontrollen der Bundespolizei in Inlandszügen

Das Verwaltungsgericht (VG) Koblenz hat mit einem Urteil vom 07.11.2014 die rechtliche Basis für Personenkontrollen der Bundespolizei in vielen Zügen grundsätzlich infrage gestellt. In dem Fall geht es um eine Klage von zwei Deutschen mit schwarzer Hautfarbe. Die Eheleute aus Mainz waren im Januar 2014 in einer voll besetzten Regionalbahn mit ihren Kindern von Mainz nach Bonn unterwegs und wurden als einzige in dem gesamten Zug von drei Bundespolizisten kontrolliert. Dies hatte auch unter weiteren Zuggästen, die sich als Zeugen zur Verfügung stellten, zu Protesten geführt.

Die Richter in Koblenz erklärten die Kontrolle nicht nur für rechtswidrig – sondern fällten eine über den Einzelfall hinausgehende Entscheidung. Das Gericht beschäftigte sich gar nicht erst mit der Frage, ob die Kontrolle diskriminierend sei, sondern bestritt grundsätzlich die Befugnisse der Bundespolizei, verdachtsunabhängige Kontrollen in den meisten deutschen Zügen durchzuführen. Die Bundespolizei stützt sich bei den Kontrollen auf § 22 Bundespolizeigesetzes (BPolG). Gemäß Absatz 1 darf die Bundespolizei zur Verhinderung von illegaler Einreise „jeden" befragen und kontrollieren. Nach Ansicht des VG Koblenz ist dies nur in Zügen zulässig,

die tatsächlich zur Einreise genutzt werden können. Und dies gelte nicht für die meisten Inlandszüge, sondern nur, wenn aufgrund von konkreten Lageerkenntnissen oder grenzpolizeilicher Erfahrung anzunehmen sei, dass der Zug zur unerlaubten Einreise genutzt werde. In Regionalzügen ohne Grenzanbindung oder Halt bei Flug- oder Seehäfen könne allenfalls eine illegale „Weiterreise“ verhindert werden. Der Gesetzeswortlaut sei daher keine gesetzliche Grundlage für verdachtsunabhängige Kontrollen in den meisten Zügen im Inland.

Rechtsanwalt Sven Adam, der die Kläger juristisch vertritt, wies darauf hin, dass das Urteil zwar nicht bindend für andere Gerichte ist. Sollte sich jedoch die Auffassung des VG durchsetzen, bedeute dies die faktische Abschaffung dieser Kontrollen zumindest in den meisten deutschen Zügen und Bahnanlagen. Die obere Instanz, das Oberverwaltungsgericht (OVG) Rheinland-Pfalz, war schon mit den Kontrollen der Bundespolizei beschäftigt. Im Oktober 2012 hatte das OVG mit einer Entscheidung für Aufsehen gesorgt, nach der die Kontrolle eines Studenten einzig wegen seiner Hautfarbe für nicht mit dem Gleichheitsgrundsatz des Grundgesetzes vereinbar erklärt worden ist. Der Bundespolizist, der die Kontrolle durchgeführt hatte, gab vor Gericht zu, dass er den Reisenden vor allem aufgrund seiner Hautfarbe kontrolliert hatte: Er spreche Leute an, „die ihm als Ausländer erschienen“. Der Betroffene sah sich in unzulässiger Weise diskriminiert. Das Gericht sah das ebenfalls so, und stellte klar, dass Kontrollen aufgrund der Hautfarbe gegen das Grundgesetz verstoßen. Weitere Klagen von Betroffenen werden derzeit behandelt.

Dass Kontrollen allein wegen der „ethnischen Herkunft“ nicht zulässig sind, ist weitgehend unumstritten. Die Bundesregierung antwortete auf eine Anfrage der Linksfraktion im Jahr 2012, die äußere Erscheinung einer Person könne „unter Umständen eines von mehreren Kriterien sein, die zu einem Handeln der Beamten führen können, niemals jedoch das alleinige Kriterium“. Die EU-Agentur für Grundrechte (Fundamental Rights Agency – FRA) hatte bereits 2009 festgestellt: „Jegliche Form des ethnischen Profiling ist auch nach internationalem Recht ungesetzlich, weil es gegen die Garantien des internationalen Übereinkommens über die Beseitigung jeder Form der Diskriminierung verstößt.“ Auch der UN-Menschenrechtsausschuss entschied, dass polizeiliche Ausweiskontrollen, die durch ethnische Herkunft begründet sind, gegen die internationalen Nichtdiskriminierungsstandards verstoßen.

Amnesty International (AI) forderte Anfang Dezember 2014 eine Reform des BPolG sowie vergleichbarer Gesetze auf Länderebene. Die Regelung im BPolG erlaube es, ohne konkreten Anlass und Verdacht „zur Verhinderung oder Unterbindung unerlaubter Einreise“ Menschen zu kontrollieren. Diese Norm provoziere geradezu dazu, Personen nach rassistischen Kriterien zu kontrollieren, was dem Grundgesetz und den Menschenrechte widerspreche (Gensing, Keine Personenkontrollen mehr in Inlandszügen?, www.tagesschau.de 07.11.2014; Amnesty kritisiert Kontrollen, SZ 02.12.2014, 6).

BSG

Chip und Passbild bei eGK zulässig

Mit Urteil vom 18.11.2014 entschied das Bundessozialgericht (BSG), dass der Computerchip und ein Passfoto auf der elektronischen Gesundheitskarte (eGK) einer Krankenkasse nicht unzulässig in das Recht der Versicherten auf informationelle Selbstbestimmung eingreifen und hat damit die Revision eines Rentners aus Fuldatal bei Kassel zurückgewiesen (Az. B 1 KR 35/13 R). Mitglieder einer Krankenkasse können danach keine Gesundheitskarte ohne Lichtbild verlangen. Hierfür gebe es keine gesetzliche Ausnahmeregelung. Es bestehe ein überwiegendes Interesse an dem durch das Bild verbesserten Schutz vor Missbrauch gegenüber dem Interesse des Einzelnen.

Der klagende Versicherte scheiterte damit endgültig mit seinem Anliegen, eine Gesundheitskarte ohne Passbild nutzen zu können. Er sah sein Grundrecht auf informationelle Selbstbestimmung dadurch verletzt, dass er nicht



nachverfolgen könne, wer die hochsensiblen Daten abrufe und verarbeite. Er monierte, dass auf dem Chip auch hochsensible medizinische Daten wie z. B. eine elektronische Patientenakte abgespeichert werden können. Das Lichtbild sei zur Identifizierung nicht nötig. Das Hessische Landessozialgericht hatte die Klage des Rentners 2013 abgewiesen.

Da die eGK mit Chip und Lichtbild gerade den Schutz vor missbräuchlicher Inanspruchnahme verbessere, sei, so urteilte das BSG, das Vorbringen des Versicherten unerheblich. Es lasse sich nicht feststellen, das die Datensicherheit, wie von ihm behauptet, tatsächlich unzulänglich sei. Man dürfe davon ausgehen, dass die geltenden Gesetze die betroffenen Daten vor unbefugtem Zugriff Dritter ausreichend schützen. Die auf der Karte gespeicherten Daten entsprächen denen auf der alten Krankenversichertenkarte. Durch den mit dem Lichtbild verhinderten Missbrauch der eGK werde die Wirtschaftlichkeit und Leistungsfähigkeit der Krankenkasse verbessert. Gestohlene oder verloren gegangene Karten könnten sofort identifiziert werden. Damit diene sie in ihrer derzeitigen Gestalt und mit ihren Funktionen dem Allgemeininteresse (Mit Chip und Passbild, SZ 19.11.2014, 6; Versicherte müssen Lichtbild dulden, www.lto.de, 19.11.2014).

Dr. Volker Hammer

Secorvo Security Consulting GmbH

Normentwurf „Leitlinie Löschkonzept“

Im Dezember 2012 stellte Secorvo die DIN-INS-Leitlinie zur „Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ vor.[1] Sie gibt Empfehlungen für die Inhalte und den Aufbau eines Löschkonzepts, sowie die Zuordnung der Verantwortlichkeiten. Der Schwerpunkt liegt auf einer effizienten Vorgehensweise zur Entwicklung von Löschregeln für Datenarten unter Verwendung von vereinheitlichten Löschklassen.

Eine einheitliche Vorgehenswese für Löschkonzepte bietet die Chance, branchenweite oder sogar branchenübergreifende Löschregeln für personenbezogene Daten festzulegen. Diese würden es Unternehmen erleichtern, angemessene Löschprozesse zu etablieren. Ende 2013 startete daher ein von den Unternehmen Blancco, DATEV, Deutsche Bahn, Secorvo und Toll Collect gefördertes Projekt, in dem die Leitlinie zu einer DIN-Norm weiterentwickelt wird. Seit dem 09.01.2015 liegt ein Entwurf der Norm 66398 auf dem Entwurfsportal des DIN vor (http://www.entwuerfe.din.de/). Die Norm soll im Herbst 2015 verabschiedet werden. Bereits der Normentwurf gibt wesentliche Hilfestellung für die Entwicklung eigener Löschkonzepte.

1 Vgl. auch Hammer, V.: Löschen nach Regeln in DANA 1/2013. Die Leitlinie ist zum Download verfügbar unter http://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf.

Buchbesprechungen



Hofstetter, Yvonne
Sie wissen alles
Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen
C. Bertelsmann, München 2014, 351 S., ISBN 978-3-570-10216-9

(TW) Der angloamerikanische Turbo-Informationskapitalismus hat noch lange nicht gesiegt, auch wenn vieles für einen solchen Ausgang spricht: die Konzentration von (Risiko-) Kapital auf das Silicon Valley/USA und zunehmend auf China, die informationelle Ausbeutung durch Unternehmen wie Google, Facebook oder Amazon, deren Ignoranz und Missachtung digitaler Grundrechte einschließlich der Würde des Menschen. Zur Maximierung von Kapital und politischer Macht wird der Mensch zum Objekt degradiert und in seiner Subjektivität verleugnet.

Nach der Autorin gibt es eine Alternative, die aber nichts mit dem kommunistischen oder einem sonstigen totalitären Kollektivismus zu tun hat. Hofstetter nennt diesen paretooptimierte soziale Marktwirtschaft. Damit versucht sie das zu benennen, was in der – viel zu wenig stattfindenden – Ideologiedebatte (noch) keinen etablierten Begriff gefunden hat. In der aufklärerischen Tradition Kants geht es um die Wahrung der Demokratie mit ihren Freiheitsverbürgungen und der Anerkennung des Individuums in seiner Würde in einer Gesellschaft, die von Big Data und totalitärer Informatisierung geprägt ist.

Inspiriert von dem im Juni 2014 verstorbenen Frank Schirrmacher verfasste die Autorin ein leidenschaftliches Plädoyer für eine Humanisierung unserer Informationsgesellschaft. Dabei verfolgt sie die Entstehung und Entwicklung des Big Data von den Ursprüngen bis zur Gegenwart und liefert dabei als Informatikerin spannende Einblicke in eine öffentlich bisher wenig durchleuchtete Technikentwicklung – die des Generierens, Fusionierens und Analysierens gewaltiger digitaler Datenmengen. Die Ursprünge gehen für sie insbesondere auf das Militär zurück. Nachdem sich Europa insofern aus ökonomischen Gründen von der Weiterentwicklung der vorhandenen Forschungskompetenzen verabschiedet hat, erfolgte ein Brain Drain in den Finanzsektor, der zum automatisierten Hochgeschwindigkeits-Börsensystem führte, das einen zentralen Beitrag leistete für mehrere Börsencrashs, u. a. zum Finanzmarktzusammenbruch 2008. Die Fortschreibung dieser Technologie

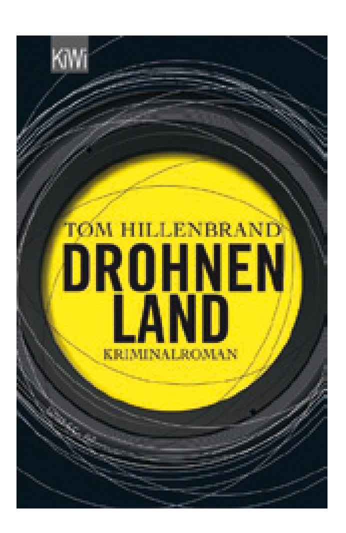
zur digitalen Ausbeutung der Menschen wird von der Autorin plausibel dargestellt, ebenso die damit verbundenen Risiken für unsere Menschenwürde, für unsere informationellen Freiheiten und für demokratische Transparenz.

Es ist äußerst erfrischend, wie hier eine Technikexpertin mit ihrem informatischen Ansatz zu Ergebnissen kommt, auf die DatenschützerInnen und BürgerrechtlerInnen schon seit Jahren hinweisen: die Gefahr einer macht- und technikgesteuerten Big-Data-Diktatur. Wie dieser Gefahr begegnet werden kann und sollte, ist schon thematisiert worden, wird hier aber nachdrücklich begründet: mit klassischen staatlichen Datenschutzinterventionen, mit Datensparsamkeit, mit dem Einfordern von Transparenz der Datenverarbeiter, mit der Normierung und Durchsetzung digitaler Grund- und Freiheitsrechte – auch auf internationaler Ebene. Aus einer ökonomischen Perspektive ergänzt sie: die Bekämpfung der digitalen Machtkonzentration durch staatliche Kartellregulierung und Technikbesteuerung. Interessant ist ihre Diagnose, weshalb insofern bisher wenig passiert ist; Hofstetter konstatiert eine hohe Technikignoranz bei der Politik, die bekämpft werden müsse und könne.

Das Buch ist zweifellos ein Sachbuch. Es liest sich aber, vor allem zum Einstieg bei der Dokumentation von militärischen und finanzwirtschaftlichen Abläufen, teilweise romanhaft und fesselnd. Es zeigt, wie – in der Tradition von Dürrenmatts Physikern – InformatikerInnen gesellschaftliche und politische Verantwortung übernehmen müssen – unter Rückgriff und im Bewusstsein unserer europäischen Wertegeschichte. Dabei vermittelt die Autorin auch für Laien ein gutes Verständnis für die Big-Data-Technik, deren Logik und deren Funktionsmechanismen, und wie diese entwickelt wurde und geeignet ist, uns unserer Freiheiten zu berauben.

Ohne die juristische Terminologie zu übernehmen, vermittelt sie angesichts der technologischen Möglichkeiten der Informatisierung unserer Gesellschaft die Antworten unseres Grundgesetzes und der europäischen Grundrechtecharta. Sie zeigt auf, welche segensreichen Wirkungen die kurz vor Manuskriptabgabe getroffene Google-Entscheidung des EuGH hat. Sie benennt aber auch, weshalb die wenig zuvor ergangene Scoring-Entscheidung des Bundesgerichtshofes, die die Geheimhaltung von uns bestimmendem Scoring-, und damit von Big-Data-Algorithmen absegnet, so falsch ist.

Hofstetter vermittelt uns die Einsicht, dass es notwendig ist und dass es sich lohnt, gegen den angloamerikanischen Turbo-Informationskapitalismus anzukämpfen, ohne dabei auf die segensreichen Errungenschaften der Informationstechnik – einschließlich des Big Data – verzichten zu müssen. Allen, denen eine humane Informationsgesellschaft ein Anliegen ist, kann dieses Buch ans Herz gelegt werden. Ein aussagekräftiges Sachverzeichnis erleichtert übrigens, nachdem man das Buch einmal gelesen hat, das spätere Auffinden wertvoller Sachinformationen.



Hillenbrand, Tom
Drohnenland
Kriminalroman
Kiepenheuer & Witsch, Köln, 2. Aufl. 2014, 423 S., ISBN 978-3-462-04662-5

(TW) Wohin führt uns die digitale Informatisierung aller Lebensbereiche? Eine mögliche und nicht ganz unwahrscheinliche Antwort hierauf gibt dieser spannende Kriminalroman. Wir tragen unsere Smartphones nicht mehr in unseren Hosentaschen, sondern als Specs, digitale Brillen, auf der Nase, die wir mit Spracheingaben steuern. Transportieren werden uns selbstfahrende Autos. Bedienen und kontrollieren werden uns Drohnen. Diese können winzig sein wie eine Mücke, Colibris oder auch große Skyships. Die spektakulärste Erfindung des Tallan Konzerns ist aber die digitale Spiegelung, mit der es möglich ist, dank einer Datenkappe auf dem Kopf und mental wirkender Pharmaka, wahrnehmungsmäßig über ein gewaltiges Datennetz an anderen Orten präsent zu sein – sinnlich wahrnehmend, als Hologramm möglicherweise sichtbar und bei Bedarf auch unsichtbar – eine phantastisches Angebot für staatliche Ermittler, natürlich für Europas Geheimdienst RR (Récuperation des Renseignements), aber auch für die Chefstrafverfolger von Europol. Ermittelt wird auch mit Hilfe eines „intelligenten" Polizeicomputers TEIRESIAS, den nicht nur der Held unseres Krimis, Aart Westerhuizen, liebevoll „Terry" (Telemetric Reenactments and Immersive Simulations of Actualities) nennt. Terry antwortet auf Sprachanfragen mit Sprachantworten unter Hinzuziehung sämtlicher verfügbarer Daten mit qualifizierter Prognosekompetenz und präziser Wahrscheinlichkeitsangabe.

Ein Abgeordneter des Europaparlaments Vittorio Pazzi, wird an einem unwirtlichen Ort erschossen, und der Hauptkommissar nimmt, assistiert von seiner Analystin Ava Bittmann, die virtuellen und analogen Ermittlungen auf. Wegen deren Brisanz – eine Verfassungsabstimmung steht bevor, bei der das Europaparlament in einer Verfassungsentscheidung auch über das Ausscheiden Großbritanniens aus der EU bestimmen soll – darf Westerhuizen auf die modernste Weiterentwicklung Terry IV zurückgreifen, die eigentlich nur dem Geheimdienst RR zu Diensten ist. Ein schneller Fahndungerfolg lässt viele Fragen offen, weshalb der Hauptkommissar und seine Analystin weiterermitteln, schließlich gegen den Willen ihrer Vorgesetzten. Dahinter steckt nicht nur eine Manipulation von Terry, sondern ein gewaltiger Skandal, der die Grundfesten der Europäischen Union erschüttert. Beteiligt sind u. a. EuropaparlamentarierInnen, die Kommissionspräsidentin, der Polizeipräfekt, ein äußerst virtuell agierender Journalist, ein Privacyaktivist und seine autonomen Freunde in Hamburg, der Chef des Technologiekonzerns Tallan...

Mehr soll von der Handlung nicht verraten werden. Sie ist an- und aufre-

gend bis zum Schluss. Unsere aktuelle Technikpolitik lässt sich in diesem Krimi spiegeln, die auf ein Drohnenland hinauslaufen könnte, in dem unsere Freiheiten von privater und von staatlicher Seite unter Einsatz von Informationstechnik massiv beeinträchtigt sind. Erschreckend und zugleich tröstlich ist, dass die weiter entwickelte Technik die individuellen Freiräume der Menschen massiv einschränkt und für Betrug, Manipulation, Diskriminierung und Machtmissbrauch genutzt wird, dass aber diese Technik auch Möglichkeiten zur Gegenwehr eröffnet, vorausgesetzt, es gibt engagiert, aufrichtig und wertegeleitet handelnde Menschen im Inner Circle. Ein zugleich beklemmendes wie inspirierendes Szenario.



Däubler, Wolfgang
Gläserne Belegschaften?
Das Handbuch zum Arbeitnehmerdatenschutz
Bund Verlag Frankfurt/Main, 6. Aufl. 2015, 724 S., ISBN 978-3-7663-6086-1

(TW) „Sollte mit einem Abschluss der Verhandlungen über die Europäische Datenschutz-Grundverordnung nicht in angemessener Zeit gerechnet werden können, wollen wir hiernach eine nationale Regelung zum Beschäftigtendatenschutz schaffen". Dieser Ankündigung im aktuellen Koalitionsvertrag auf Bundesebene (DANA 1/2014, 18) folgten bisher keine politischen Aktivitäten. Die Entwürfe der Grundverordnung (EU-DSGVO) machen allenfalls allgemeine Vorgaben zum Beschäftigtendatenschutz, so dass ein nationaler Regelungsrahmen erhalten bleiben wird. Es besteht jedoch nicht im Ansatz die begründete Hoffnung, dass mit den Ausführungen des Koalitionsvertrages Ernst gemacht würde. Umso wichtiger war und ist eine konsistente Darstellung der Rechtslage unter Bezugnahme auf die Rechtsprechung und die aktuelle Literatur.

Dazu legt Wolfgang Däubler nun eine neue, die 6. Auflage vor. Die „gläsernen Belegschaften" sind schon seit vielen Jahren eines der wichtigsten Standardwerke zum Arbeitnehmerdatenschutz. Sein Wert besteht darin, dass ein ausgewiesener Wissenschaftler mit praktischen Erfahrungen arbeitnehmerfreundliche und damit auch datenschutzfreundliche Auslegungen im Beschäftigtendatenschutz bereitstellt. Dieser Bereich ist in der Praxis massiv umkämpft. Es bestehen antagonistische Interessen – der Arbeitgeber auf möglichst weitgehende und der Arbeitnehmer auf möglichst eingeschränkte Kontrolle. Bei aller Parteilichkeit schafft es Däubler, gute Vorschläge für einen Ausgleich zu machen, die beiden Seiten gerecht werden. Letztendlich nützt ein professioneller Datenschutz im Unternehmen beiden Seiten und bindet die Beschäftigten an das Unternehmen.

Die Beschäftigtenkontrolle unterliegt einer rapiden technischen Entwicklung in den Unternehmen, bei der auf die modernen Mittel von vernetzten Rechnern, Smartphones und sonstige Mobilgeräte, Video, Biometrie, Clouddatenverarbeitung und Internet eingesetzt werden. Dabei ist von größter Bedeutung, dass diese technische Realität durch Betriebsvereinbarungen und die Tätigkeit der Betriebsräte eingegrenzt wird. Hierzu geben die „gläsernen Belegschaften" die nötigen hilfreichen rechtlichen Hinweise. Auch die einzelne ArbeitnehmerIn findet die nötigen Hilfen, wie sie sich individualrechtlich gegen übermäßige Kontrolle und Bevormundung durch den Arbeitgeber zur Wehr setzen kann. Entsprechendes gilt für die Kontrolltätigkeit von betrieblichem Datenschutzbeauftragten und Aufsichtsbehörden. Das Buch bleibt auf keine aktuelle relevante Frage eine Antwort schuldig und verweist durch umfassende Nachweise auf die Literatur und Rechtsprechung zu den jeweiligen Fragestellungen. Ein umfassendes Stichwort- und Literaturverzeichnis macht dieses Standardwerk zum unverzichtbaren Hilfsmittel beim Arbeitnehmerdatenschutz in Wissenschaft und Praxis, gerne auch für die Praxis der nationalen Gesetzgebung.

(ks) Wolfgang Däublers „Gläserne Belegschaften" gehört zu den Standardwerken des Arbeitnehmerdatenschutzes. Das Werk wird nicht nur von Betriebs- und Personalräten seit vielen Jahren regelmäßig zu vielen betrieblichen Fragestellungen konsultiert. Umso erfreulicher ist es, dass nun eine überarbeitete Auflage zur Verfügung steht, die die neueste Gesetzeslage und Rechtsprechung bis einschließlich 2014 auswertet.

Der Autor weist bereits im Vorwort auf Neuerungen hin, die erstmals Eingang gefunden haben: Cloud Computing, Big Data, Auslagerung von Aktivitäten ins Internet und der betriebliche Umgang mit Facebook sind hierbei nur einige Stichworte.

Die altbekannten Fragestellungen werden gleichwohl weiterhin erörtert: Ob und unter welchen Bedingungen der Chef die E-Mails seiner Beschäftigten lesen darf, gehört ebenso dazu, wie die Rahmenbedingungen, unter denen Videoüberwachung statthaft sein kann.

Zwei große Stärken kennzeichnen das Werk, die besonders ins Auge stechen: Dem Autor gelingt eine ebenso systematische wie praxisnahe Darstellung wesentlicher betrieblicher Datenschutz-Fragestellungen. Und er integriert die ausführliche Würdigung gerichtlicher Entscheidungen, ohne deren Kenntnis die Gesetzeslage gerade für juristische Laien häufig nur schwer interpretierbar erscheint.

Nach einleitenden Kapiteln zur Erläuterung der datenschutzrechtlichen Grundlagen des Arbeitnehmerdatenschutzes und seinen Auswirkungen auf das Arbeitsrecht, arbeitet sich der Autor systematisch durch die Zulässigkeitsgrundlagen der Datenerhebung und -verarbeitung von Bewerbern, Beschäftigten und ausscheidenden Mitarbeitern. Eigene Kapitel werden der Auswertung dieser Daten, also der Nutzung im datenschutzrechtlichen Sinne, der Übermittlung im Inland sowie ins Ausland gewidmet. Schließlich werden Fragen der Transparenz (als Voraussetzung für persönliche Kontrollmöglichkeit)

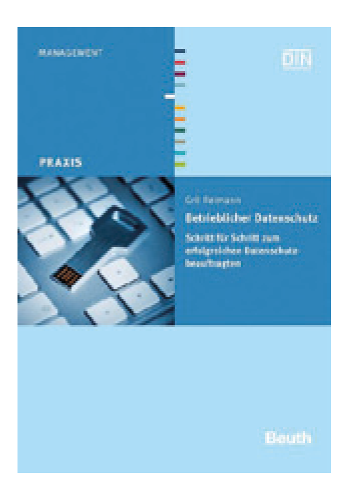
erörtert und die daraus resultierenden Individualrechte und kollektiven Kontroll- und Mitbestimmungsrechte durch Betriebs- oder Personalräte. Der Blick auf die Zugriffsmöglichkeiten staatlicher Organe runden die Darstellung ab.

Viele Themen werden in dieser Auflage erstmals oder wesentlich ausführlicher als in der Vorauflage erörtert. So zum Beispiel die Fragen rund um Tätigkeiten der internen Revision und von Compliance-Abteilungen. Däubler beschreibt, unter welchen Rahmenbedingungen Korruptionsbekämpfung und Abwehr sonstigen rechtwidrigen Verhaltens zulässig sind und wo das Persönlichkeitsrecht von Beschäftigten allzu ungehemmte Auswertungen verbietet.

Die Chance auf systematische Erörterung von Problemen rund um Cloud Computing wurde allerdings (noch?) nicht ergriffen. Zwar widmet sich ein Abschnitt der Problematik in Zusammenhang mit der Erteilung von Auftragsdatenverarbeitung bzw. Übermittlung von Arbeitnehmerdaten ins Ausland, aber konkrete Anwendungsbezüge sucht man vergebens. Auch im Kapitel „Ungelöste Probleme“ wird das Cloud Computing eher als unbeherrschbare Konstruktion dargestellt ohne auf die Bandbreite der unterscheidbaren Cloud Computing-Lösungen einzugehen oder Haltungen von Aufsichtsbehörden und Artikel-29-Gruppe zu hinterfragen. Angesichts der gerade aktuellen Diskussionen, z.B. über Office365, sehr schade!

In manchen Detailfragen erscheinen Empfehlungen oder Darstellungen auch praxisfremd. So wirkt die Feststellung, dass es dem Arbeitnehmer unbenommen sei, seine E-Mails zu verschlüsseln, davon jedoch nur sehr eingeschränkt Gebrauch gemacht werde, für den in größeren Unternehmen tätigen Praktiker etwas befremdlich. Schon allein aus Sicherheitsgründen verhindern unzählige Unternehmen zu Recht, dass Beschäftigte Software-Installationen vornehmen können, geschweige denn individuell über den Einsatz von Verschlüsselungslösungen entscheiden können. Auch wenn die Argumentation – das Verbot der Verschlüsselung würde, wie das Verbot der Verwendung von Briefumschlägen, die Persönlichkeitsrechte der Beschäftigten verletzen – sympathisch erscheint: Nicht ein individuelles Entscheidungsrecht des Beschäftigten kann abgeleitet werden, sondern vielmehr die Pflicht des Unternehmens, dem Beschäftigten eine Verschlüsselungsmöglichkeit bereitzustellen. Diese kann dann aber dem Unternehmens-Sicherheitsstandard entsprechend installiert werden.

Trotz der beispielhaft genannten, kleineren Schwächen, ist das Handbuch eine unverzichtbare Quelle für die Darstellung wesentlicher Aspekte und Fragestellungen des Beschäftigtendatenschutzes. Insgesamt erhalten sowohl Datenschutzbeauftragte als auch Betriebs- und Personalräte ein umfassendes Nachschlagewerk für die alltäglichen Datenschutzaufgaben.



Grit Reimann
Betrieblicher Datenschutz – Schritt für Schritt zum erfolgreichen Datenschutzbeauftragten
Beuth-Verlag, 2013, 1. Auflage
ISBN 978-3-410-22760-1
EUR 56,00

(ks) Neu bestellte Datenschutzbeauftragte suchen häufig nach Literatur, die ihnen den Einstieg in ihr Amt erleichtert. Welche Aufgaben sind vorrangig zu bearbeiten? Welche Abläufe sind zu beachten? Wo finde ich weiterführende Literatur?

Grit Reimann hat als Beraterin für Umweltmanagement, betriebliches Gesundheitsmanagement, Energiemanagement, Qualitätsmanagement und Datenschutz mit Sicherheit große Erfahrung beim sinnvollen und effizienten Organisieren betrieblicher Abläufe. Und so vermittelt das Inhaltsverzeichnis ihres Leitfadens für Datenschutzbeauftragte auch durchaus die Übersicht über viele wichtige Themen, die einen frisch ins Amt gestarteten Datenschutzbeauftragten interessieren: Fragen rund um die Person und die Aufgaben des Amtsinhabers, zu technischen und organisatorischen Maßnahmen, zu sinnvollen betrieblichen Regelungen und Verträgen und nicht zuletzt zur Durchführung von Schulungen.

Über die Reihenfolge der Behandlung ließe sich streiten, aber letztlich ist es Geschmackssache, ob man Einzelfragen wie den Umgang mit Auftragsdatenverarbeitung oder Datenschutz im Personalwesen diskutiert, bevor man Empfehlungen zu Grundsatzfragen wie der organisatorischen Verankerung des Datenschutzes mittels Datenschutzkonzept oder Datenschutzhandbuch erteilt.

Was allerdings keine Geschmackssache ist, sind die vielen Ungenauigkeiten, die den ratsuchenden Neuling in die Irre führen. So wird behauptet, dass die Bestellung des Datenschutzbeauftragten keinem Beteiligungsrecht des Betriebsrats unterliege, was zumindest dann nicht stimmt, wenn die Bestellung mit einer Versetzung oder Einstellung einhergeht, was in nicht wenigen Fällen zutreffen dürfte. Die Erörterung der Besonderheiten externer Datenschutzbeauftragter und deren Einbindung fehlen völlig. Als lediglich „nicht empfehlenswert“ wird die Bestellung von Personen aus der IT-Leitung oder der Personalleitung bezeichnet. Dass eine solche Bestellung schlichtweg unzulässig wäre, wäre die korrekte Darstellung gewesen. Richtiggehend falsch wird es, wenn der Datenschutzbeauftragte für die Einhaltung des Datenschutzes und die ordnungsgemäße Anwendung der Datenverarbeitung verantwortlich gemacht wird. Dass die Verantwortung nach wie vor bei der Unternehmensleitung liegt und der DSB keinerlei Durchsetzungsmöglichkeiten für seine Empfehlungen hat, wäre die korrekte Darstellung gewesen.

Die Rolle und Handhabung von Zulässigkeitsgrundlagen werden an mehreren Stellen zumindest verwirrend dargestellt. Besonders deutlich wird dies im Abschnitt über die Beurteilung der Reisedatenerhebung. Dass der Arbeitsvertrag hierfür nicht Grundlage

sein kann, wird nur angedeutet, aber nicht begründet. Stattdessen wird empfohlen, eine in Dienstreiseanträge integrierte Einwilligung der Reisenden einzuholen. Unabhängig davon, dass eine Einwilligungserklärung, die mangels fundiert ermittelter Zulässigkeitsgrundlage „sicherheitshalber“ eingeholt wird, nicht zulässig ist, bleibt vollkommen unklar, was passieren soll, wenn ein Reisender seine einmal erteilte Einwilligung später zurückzieht. Dass dies möglich sein muss, ist Grundlage einer wirksamen Einwilligung und als Konsequenz muss der zugehörige betriebliche Prozess eine angemessene Behandlung der auf Grundlage der Einwilligung verarbeiteten Daten vorsehen. Diesen Aspekt vergisst die Autorin auch bei weiteren Gestaltungsvorschlägen, die auf Einwilligungen beruhen sollen.

Endgültig unzulässig wird es, wenn zu Durchführung bestimmter gesundheitspräventiver Maßnahmen eine Entbindung der Betriebsärzte von ihrer Schweigepflicht allein durch Betriebsvereinbarung empfohlen wird. Dass es sich bei der ärztlichen Schweigepflicht nicht um eine Datenschutz- sondern um eine Strafvorschrift handelt, die nicht durch BV ausgehebelt werden kann, verkennt die Autorin offenbar vollständig.

Leider finden wesentliche Aspekte des Datenschutzes in gar keiner Weise Erwähnung. Die Rolle grundlegender Prinzipien wie Zweckbindung, Erforderlichkeit mit Datensparsamkeit und Datenvermeidung sowie Transparenz wird nicht thematisiert. Da wundert dann auch nicht, dass der wichtige Aspekt der Löschung von Daten und dessen Organisation vollkommen ausgeblendet wird.

Schade auch, dass die Lücken nicht wenigstens durch Empfehlungen zu weiterführender Literatur geschlossen werden. Es gibt weder Literatur- oder Empfehlungsliste noch einen Index zur Erschließung des Inhalts.

Mehr als eine erste Orientierung kann das Werk Neulingen nicht bieten. Die inhaltlichen Detailaussagen zu datenschutzrechtlichen Aspekten sind mit äußerster Vorsicht zu genießen. Praktikern ist unbedingt eine Verifizierung durch ergänzendes Literaturstudium oder sonstige verlässliche Quellen zu empfehlen.



Christoph Bausewein
Legitimationswirkung von Einwilligung und Betriebsvereinbarung im Beschäftigtendatenschutz
Diss. Universität Oldenburg 2011
Oldenburger Verlag für Wirtschaft, Informatik und Recht, Edewecht, 2012
ISBN 978-3-939704-67-6
EUR 49,80

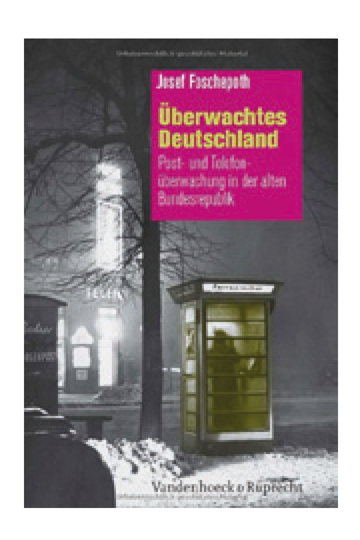
(ks) Welche Themen geeignet sind und wie Betriebsvereinbarungen gestaltet sein müssen um Zulässigkeitsgrundlage für eine automatisierte Datenverarbeitung Beschäftigter sein zu können, wird seit Jahren kontrovers diskutiert. Noch schärfer wird die Auseinandersetzung darüber geführt, ob überhaupt und wenn ja, unter welchen Voraussetzungen, ein Arbeitgeber gültige Einwilligungen seiner Beschäftigten zur Legitimierung automatisierter Datenverarbeitung einholen kann.

Christoph Bausewein hat sich in seiner lesenswerten Dissertation diesen Fragen nicht nur von der theoretisch-juristischen Seite genähert, sondern anhand verbreiteter Anwendungsfälle auch die praktische Auswirkung der rechtssystematischen Erkenntnisse dargestellt.

Nach einer Betrachtung der historischen Entwicklung des Beschäftigtendatenschutzes widmet er das Hauptkapitel der Darstellung und Bewertung von Rechtsquellen. Neben den grundsätzlich bekannten Prinzipien des Datenschutzes werden hier auch sonstige grundlegende Rechte beider Seiten, Arbeitnehmer und Arbeitgeber, erörtert. Dass der Autor dabei aus dem vom BverfG manifestierten Schutz der „Integrität und Vertraulichkeit informationstechnischer Systeme“ kurzerhand „informatorische Systeme“ macht, kann man verschmerzen. Auch die Rechtsstellung von Betriebsvereinbarungen wird untersucht und eingeordnet.

Im dritten Kapitel wendet der Autor seine Erkenntnisse auf ausgewählte betriebliche Fragestellungen an. So untersucht er die Zulässigkeit von Internetrecherchen in Bewerbungsverfahren, die Durchführung medizinischer Einstellungsuntersuchungen, die Durchführung von Persönlichkeitstests. In Bezug auf ein umfassendes und permanentes Gesundheitsmonitoring mit Erfassung medizinischer Werte (Atmung, Herzfrequenz etc.) kommt er beispielsweise zu dem Schluss, dass es wegen grober Verletzung der Menschenwürde weder durch Einwilligung noch durch Betriebsvereinbarung rechtmäßig gestaltet werden könne. Dies ist umso bemerkenswerter als er ansonsten die Meinung nicht teilt, dass eine Einwilligung im Arbeitsverhältnis kaum wirksam eingeholt werden könne.

Die Arbeit enthält zudem eine umfangreiche Literatur- und Entscheidungssammlung und ist, wenngleich in erster Linie als wissenschaftliches Werk verfasst, auch für den betrieblichen Praktiker durchaus wertvoll.



Josef Foschepoth
Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik
Verlag Vandenhoeck & Ruprecht
4. Auflage, 2013, 377 Seiten
ISBN: 978 3 525 30041 1, 34,99 Euro
ISBN: 978 3 647 30041 1, 27,99 Euro (E-Book)

(rp) Im Rahmen einer konzertierten Aktion von Bundesarchiv und Histori-

kerverband und Dank tatkräftiger Vorarbeit und Unterstützung seitens der Medien, insbesondere des Spiegels und der FAZ, gelang es, die Bundesregierung zu einer Neuregelung der so genannten „Verschlusssachenanweisung“ (VSA) zu bewegen, die die Freigabe von Geheimakten im Interesse von Forschung und Öffentlichkeit neu regeln sollte. Auf Vorschlag des damaligen Bundesinnenministers Wolfgang Schäuble beschloss das Bundeskabinett am 16. September 2009, die VS-Akten schrittweise freizugeben. Der Autor, Prof. Foschepoth, ist der erste und bisher einzige Wissenschaftler, der Zugang zu diesen Akten hatte. Das Ergebnis seiner Recherche hat er in dem vorliegenden Buch zusammengefasst – einschließlich der am Ende abgedruckten „Quellen-Dokumentation“, etwa 90 Seiten, in denen die wichtigsten Dokumente inhaltlich wiedergegeben werden.

Das Buch beginnt als Ausgangssituation 1945 mit der bedingungslosen Kapitulation Deutschlands. Deutschland hatte danach weder eine Regierung, noch eine gültige Verfassung und wurde zunächst von den Siegermächten regiert – und überwacht. Ein gemeinsames Ziel der Siegermächte war, ein Wiederaufleben der deutschen Gefahr ein für alle Mal zu verhindern. So weit so gut, was sicher auch aus heutiger Sicht nachvollziehbar ist.

Der schon sehr bald einsetzende Kalte Krieg führte dazu, dass der Osten (später DDR) von der Sowjetunion regiert und überwacht wurde, der Westen (später BRD) von den Westmächten. Die Überwachung im Osten ist hinlänglich bekannt und daher kein großes Thema dieses Buches. Bisher weniger bekannt ist jedoch, dass auch im Westen ein kaum für möglich gehaltenes Überwachungssystem aufgebaut wurde. Das Buch beschreibt detailliert die einzelnen Schritte des Aufbaus sowohl der tatsächlichen Überwachung als auch der Rechtsgrundlagen dafür, die – man kann es kaum glauben – größtenteils geheim gehalten wurden.

Mit Blick auf die doppelte Gefahr bedurfte es einer Strategie, die beide Gefahren gleichzeitig unter Kontrolle brachte, einer „Strategie der doppelten Eindämmung“. Darunter wurde zum einen die Eindämmung der Sowjetunion durch „Gegenmachtsbildung in Westeuropa“, zum anderen die Eindämmung Westdeutschlands durch Integration in die westliche Bündnisstruktur verstanden. Schon bald kamen die Westmächte zu dem Schluss, dass es sehr viel effizienter wäre, die Überwachung nicht vollständig selbst zu übernehmen, sondern auch die Westdeutschen, mit Hilfe von noch zu gründenden Geheimdiensten, mit einzubinden.

Im Buch werden die daraus folgenden Einzelschritte beschrieben (und belegt), durch welche die neuen Dienste (BND, BfV, Landesämter für Verfassungsschutz und weitere) verpflichtet wurden, auf Weisung der Alliierten tätig zu werden und die Ergebnisse der Überwachungen direkt an diese weiterzuleiten.

Mit Inkrafttreten des Grundgesetzes 1949 schien eine Überwachung durch deutsche Stellen nicht möglich zu sein (Art. 10 GG) und tatsächlich war die (trotzdem) stattfindende Überwachung unter Beteiligung vieler deutscher Stellen bis 1968 verfassungswidrig. Beschrieben werden im Buch die Konflikte, mit denen die vielen an dieser Überwachung beteiligten Beamten konfrontiert waren. Speziell aus dem Postministerium gab es durch den jeweils amtierenden Minister jahrelang Druck im Kabinett, diese verfassungswidrige Praxis zu beenden, indem sie sowohl durch konkrete Gesetze als auch durch eine dazu erforderliche Grundgesetzänderung legalisiert werden sollte.

Das Problem war, dass eine Gesetzesänderung und erst recht eine Verfassungsänderung nicht geheim gehalten werden konnte. Beschrieben wird im Buch ein Prozess, der sich über viele Legislaturperioden hinzog. Es musste ein Weg gefunden werden, durch den die Verfassung minimal, aber trotzdem im Sinne der Überwachung entscheidend geändert wurde, so dass die dann daraufhin neu zu verabschiedenden Gesetze mit dieser geänderten Verfassung im Einklang waren, ohne dass jedoch erkennbar wurde, worum es eigentlich ging.

Durch die Verabschiedung der sogenannten Notstands- und der G 10-Gesetze, (die sich auf das in Artikel 10 GG verankerte Grundrecht des Brief-, Post- und Fernmeldegeheimnis beziehen) sowie die damit verbundene, faktische Aufhebung der Gewaltenteilung und die dafür erforderliche Änderung des Artikels 10 GG selbst wurde die Überwachungspraxis legalisiert – und nicht erst eingeführt.

Der Autor erläutert, dass die laut Verfassung „unveränderlichen Grundrechte“, die in ihrem „Wesensgehalt“ nicht einmal mit einer ⅔-Mehrheit geändert werden können, doch grundsätzlich aufgeweicht wurden. Der schwierige Weg dahin, die Strippenzieher und auch die anschließenden Verfahren vor dem Bundesverfassungsgericht und dem Europäischen Gerichtshof, über welche die Verfassungsmäßigkeit der Gesetze und der Verfassungsänderung selbst zunächst in Frage gestellt, dann aber jeweils bestätigt wurden und die Umstände, unter denen das geschah, werden im Buch ausführlich beschrieben. Allein das enthält genug Material für einen spannenden Politthriller – obwohl es sich bei dem Buch um eine wissenschaftliche Analyse und Zusammenfassung der eingesehenen Dokumente handelt.

Es bleibt dem Leser überlassen, was er schwerwiegender einschätzt:

- den bis 1968 fortgesetzten Verfassungsbruch oder
- die dann mit der über die nötige ⅔-Mehrheit verfügenden ersten großen Koalition durchgeführte „Legalisierung“ der Überwachung, deren Umsetzung aber trotzdem weiterhin geheim gehalten wurde.

Auf die Frage, ob sich die Situation im Laufe der Jahre und spätestens mit der Wiedervereinigung 1990 in Bezug auf die Überwachungspraxis geändert hat, gibt der Autor eine klare Antwort – Nein.

Wörtlich: „Selbst bei den Zwei-plus-Vier-Verhandlungen (1990) konnte eine Aufhebung der im Zusatzvertrag zum NATO-Truppenstatut und in den Verwaltungsvereinbarungen zum G 10-Gesetz formulierten Sonderrechten der drei Mächte nicht erreicht werden. Sie bestehen bis heute fort.“

Das galt auch für alle vorhergehenden Verträge, bei denen Deutschland nach 1945 mehr Souveränität eingeräumt wurde. Es wurde immer strikt darauf geachtet, dass es verbindliche (oft geheime) Verträge gab, die den drei Westmächten (einschließlich den unter deren Auftrag agierenden deutschen Diensten) die bisherigen Überwachungsmöglichkeiten weiter unbegrenzt zusicherte.

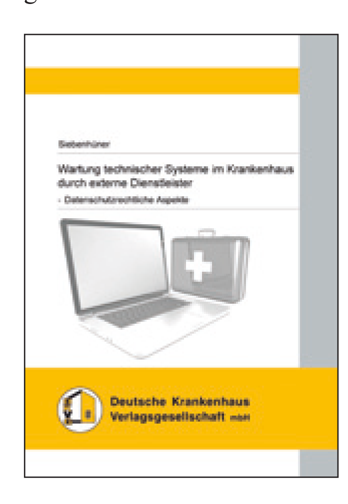
Wörtlich: „Aus Siegerrecht wurde Besatzungsrecht, aus Besatzungsrecht wur-

de Vorbehaltsrecht, aus Vorbehaltsrecht wurde deutsches Recht und gesetzliche Verpflichtung der Bundesregierung, den Post- und Fernmeldeverkehr in der Bundesrepublik durch individuelle und allgemeine Überwachungsmaßnahmen auf Wunsch und im Interesse der Alliierten zu überwachen.“

Fazit

Das Buch ist eine wichtige Lektüre für alle Interessierten, die nicht nur beispielsweise den maximalen Abstand einer Kamera von einer Hauswand korrekt beantworten wollen, sondern sich auch für den Stand der rechtlich abgesicherten tatsächlichen Überwachung interessieren, weil man sich ohne dieses Hintergrundwissen über die falschen Nachrichten empört und auch die falschen Forderungen an die Politik stellt, welche die aktuelle Situation verändern sollte.

Abschließend hierzu ein Beispiel: Weder die Einstellung des Safe-Harbor -Abkommens, noch die Forderung nach einer EuroCloud und erst recht nicht die nach einer deutschen Cloud hilft etwas, solange die deutschen Dienste selbst alles überwachen dürfen und ggf. auf Weisung z. B. der NSA auch müssen und die Ergebnisse dann vertrags- und verfassungsgemäß übermitteln.



Raik Siebenhüner
Wartung technischer Systeme im Krankenhaus durch externe Dienstleister
Deutsche Krankenhaus Verlagsgesellschaft mbH, Düsseldorf, 2013, 1. Auflage
ISBN 978-3-942734-49-3
EUR 19,90

(ks) Jeder Datenschützer, der im medizinischen Bereich tätig ist, kennt den Konflikt: Ohne externe Unterstützung kommt kaum eine IT-Abteilung aus, aber das Patientengeheimnis verbietet Externen streng genommen jegliche Tätigkeit, bei der eine Einsichtnahme in Patientendaten nicht ausgeschlossen werden kann. Selbst wenn durch Verträge und Verpflichtungen eine datenschutzrechtlich einwandfreie Konstellation besteht: die ärztliche Schweigepflicht lässt sich mit der Beauftragung externer IT-Spezialisten nicht vereinbaren. Dieser Konflikt ist dem Gesetzgeber lange bekannt; Abhilfe durch gesetzliche Klarstellung hat er bisher nicht geschaffen.

Beispiele und Konstellationen in denen dieser Konflikt praktisch gelöst werden muss, gibt es unzählige. Von der juristischen Auslagerung des Krankenhauslabors an einen externen Betreiber über die Betreuung der gesamten IT durch eine ausgelagerte Service-GmbH bis hin zur Fernwartung von Analysegeräten (auf denen sich Patientendaten befinden) durch den Hersteller.

Raik Siebenhüner hat sich dieses Themas angenommen und will neben der rechtlichen Bewertung Lösungsansätze für die rechtskonforme Umsetzung darstellen. Dies wäre sehr verdienstvoll, denn obwohl der Titel des 79 Seiten starken Bändchens die Situation im Krankenhaus in den Blick nimmt, betrifft der Grundkonflikt ebenso andere Organisationen der Gesundheitsvorsorge wie Medizinische Versorgungszentren, medizinische Labore, ja selbst niedergelassene Ärzte.

Leider hält das Werk nicht, was der Titel verspricht. Nur auf den letzten zehn Seiten ist überhaupt ein konkreterer Bezug zur Fragestellung erkennbar. Nachdem auf den Seiten zuvor abstrakt-juristisch die geltenden Gesetzesgrundlagen und deren Anwendbarkeit abgeleitet und erörtert werden, erwartet man anschließend eigentlich eine Bezugnahme auf die im Titel aufgeworfene Fragestellung. Wenn der Herleitung, dass im Krankenhaus auch Sozialdaten verarbeitet werden, alleine 6 Seiten gewidmet werden, so darf man wohl erwarten, dass diese Erkenntnis wenigstens anschließend in konkreten Zusammenhängen verwendet wird.

Allerdings endet die Schrift, ohne die erarbeiteten Erkenntnisse in praktische oder auch nur konkrete Fragestellungen des Klinikalltags zu übertragen.

Wer zum Beispiel auf Hinweise zur Rolle, Rechtmäßigkeit und Gestaltung von ADV-Aufträgen gehofft hatte, hofft vergebens. Auch die unterschiedlichen, in der Praxis anzutreffenden Arten externer EDV-Dienstleitung im Krankenhaus werden nicht thematisiert. Es ist eben nicht damit getan, alles unter „Wartung“ zu subsummieren und diesen Begriff dann auch noch mittels einer Norm zu definieren, die sich der Instandhaltung von Produktionssystemen widmet und daher äußerst ungeeeignet für den besprochenen Bereich ist.

Mangelnde technische und IT-organisatorische Kenntnisse schimmern an vielen weiteren Stellen durch, so z.B. bei der Annahme, es gebe in Bezug auf den Patientendatenschutz keinen Grund zwischen der Wartung vor Ort und der Fernwartung zu unterscheiden. Eine Feststellung, die man nur kopfschüttelnd quittieren kann. Ebenso kurios erscheint die Feststellung, dass verschlüsselte Patientendaten nicht unter das Datenschutzrecht fielen.

Wie verschlüsselte Daten denn überhaupt zustande kommen und ob sie vielleicht überhaupt erst durch Administrations- oder Wartungsvorgänge von Dienstleistern hergestellt werden können und wie dann damit konkret zu verfahren ist, wird alles nicht thematisiert.

Als Nachweis der formalen Beherrschung juristischer Herleitungssystematik mag das Bändchen wohl dienen. Als datenschutzrechtliche Hilfestellung für Fragestellungen im Krankenhaus eher nicht.

eBook-Sonderaktion für Leser der Datenschutz Nachrichten

Freihandelsabkommen TTIP. Alle Macht den Konzernen?

von Christian Felber



Freihandelsabkommen TTIP
Alle Macht den Konzernen?
73 Seiten, 3,99 €
ISBN 978-3-446-24801-4
Hanser Box,
nur als E-book verfügbar

EU und USA verhandeln seit Juli 2013 über einen transatlantischen Binnenmarkt: TTIP. Die »größte Freihandelszone der Welt« soll den Wohlstand mehren, verhandelt wird unter Ausschluss der Öffentlichkeit. Die Agenda machen die Konzerne: Sie wollen Regulierungsunterschiede beseitigen – bei Gesundheit, Verbraucherschutz, Arbeitsstandards, kultureller Vielfalt, Nachhaltigkeit. Zudem verlangen die Lobbys Fesseln für die Politik: Regeln sollen vorschreiben, wie demokratisch gewählte Gemeinderäte, Landtage und Parlamente regulieren dürfen. Obendrauf erhalten die Konzerne ein direktes Klagerecht gegen Staaten. Was als »Freihandel« verkauft wird, entpuppt sich mehr und mehr als Handelsdiktatur. Der Widerstand wächst.


Foto: Robert Gortana

Christian Felber – Buchautor, Lektor an der Wirtschaftsuniversität Wien, Initiator der „Gemeinwohl-Ökonomie“ und des Projekts „Bank für Gemeinwohl“, Österreich. Mehrere Bestseller, der Titel „Geld. Die neuen Spielregeln“ wurde als Wirtschaftsbuch des Jahres 2014 ausgezeichnet.

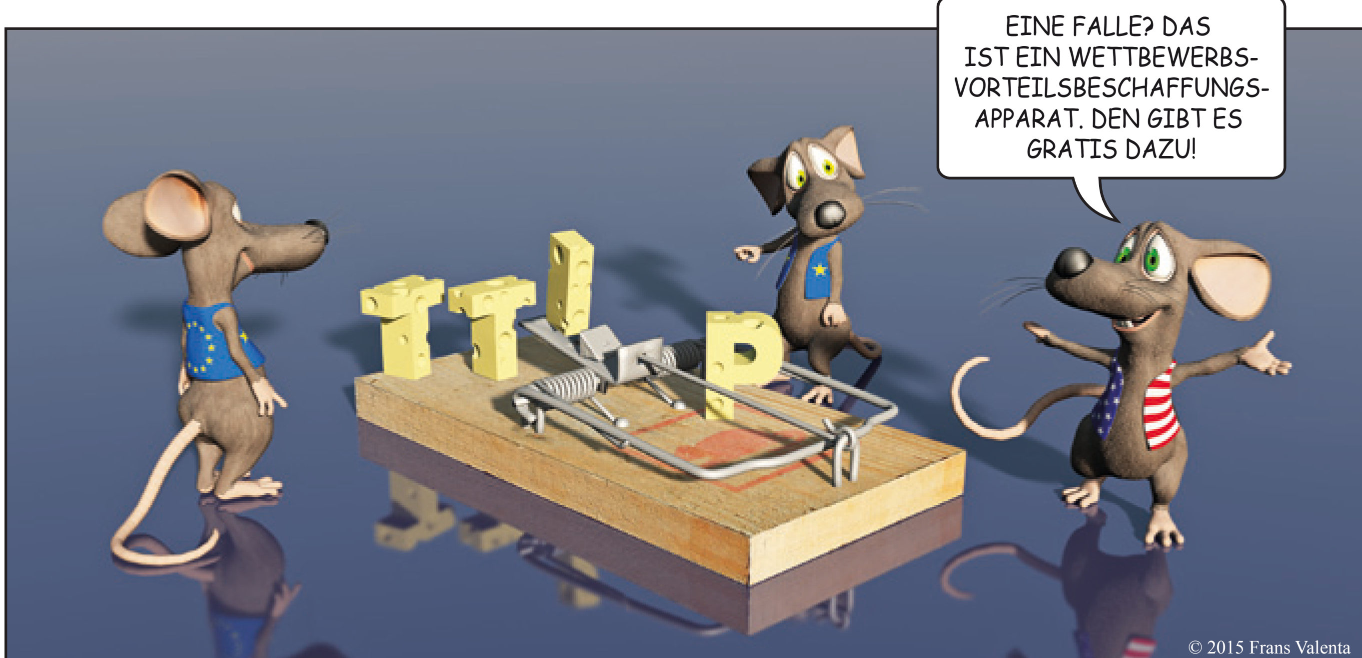
Unsere LeserInnen können das Buch bis 30. April 2015 kostenlos downloaden und lesen.

Wie geht das das?

- gehen Sie auf www.hanser-literaturverlage.de/ttip-hanserbox
- oder scannen Sie mit dem Smartphone den QR-Code
- geben Sie den Freischaltecode “TTIP” ein
- führen Sie Ihre Emailadresse an und Sie erhalten einen Downloadlink für das Buch



Cartoon



P ivat phär

Gleich ei

Brüd rlichke t

Fre h it

sicherheit

Re t

Grafik: Frans Valenta